

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF OHIO  
EASTERN DIVISION AT CLEVELAND**

|                             |   |                                |
|-----------------------------|---|--------------------------------|
| IN RE: SONIC CORP. CUSTOMER | § | MDL Case No. 1:17-md-02807-JSG |
| DATA BREACH LITIGATION      | § |                                |
|                             | § | JUDGE JAMES S. GWIN            |
| THIS DOCUMENT RELATES TO:   | § |                                |
| ALL CASES                   | § |                                |

**PLAINTIFFS' AMENDED CONSOLIDATED CLASS ACTION COMPLAINT**

William B. Federman  
Carin L. Marcussen  
FEDERMAN & SHERWOOD  
10205 N. Pennsylvania Ave.  
Oklahoma City, OK 73120  
Telephone: (405) 235-1560  
Facsimile: (405) 239-2112  
wbf@federmanlaw.com  
clm@federmanlaw.com

*Interim Lead Counsel*

Thomas A. Zimmerman, Jr.  
ZIMMERMAN LAW OFFICES, P.C.  
77 W. Washington Street, Suite 1220  
Chicago, IL 60602  
Telephone: (312) 440-0020  
Facsimile: (312) 440-4180  
tom@attorneyzim.com

*Member of Plaintiffs' Steering Committee*

Michael Fuller  
OLSEN DAINES  
US Bancorp Tower  
111 Southwest 5th Ave, Suite 3150  
Portland, OR 97204  
Telephone: (503) 201-4570  
Facsimile: (503) 362-1375  
michael@underdoglawyer.com

*Member of Plaintiffs' Steering Committee*

Marc E. Dann (0039425)  
Brian D Flick (0081605)  
DANNLAW  
P.O. Box 6031040  
Cleveland, OH 44103  
Telephone: (216) 373-0539  
Facsimile: (216) 373-0536  
notices@dannlaw.com

*Interim Liaison Counsel*

Melissa R. Emert  
STULL, STULL, & BRODY  
6 East 45th Street  
New York, NY 10017  
Telephone: (954) 341-5561  
Facsimile: (954) 341-5531  
memert@ssbny.com

*Member of Plaintiffs' Steering Committee*

Miles N. Clark  
KNEPPER & CLARK LLC  
10040 W. Cheyenne Ave., Suite 170-109  
Las Vegas, NV 89129  
Telephone: (702) 825-6060  
Facsimile: (702) 447-8048  
miles.clark@knepperclark.com

*Member of Plaintiffs' Steering Committee*

**TABLE OF CONTENTS**

|       |  |     |
|-------|--|-----|
| I.    | INTRODUCTION .....   | 1   |
| II.   | JURISDICTION AND VENUE .....                                     | 3   |
| III.  | THE PARTIES.....   | 4   |
|       | A.    PLAINTIFFS .....   | 4   |
|       | B.    DEFENDANTS .....   | 17  |
| IV.   | STATEMENT OF FACTS .....   | 18  |
| V.    | CLASS ALLEGATIONS .....  | 32  |
|       | A.    NATIONWIDE CLASS .....                                     | 32  |
|       | B.    STATEWIDE CLASSES.....                                     | 32  |
|       | C.    CERTIFICATION OF THE PROPOSED CLASSES IS APPROPRIATE ..... | 34  |
| VI.   | CAUSES OF ACTION .....   | 38  |
|       | COUNT I – NEGLIGENCE .....                                       | 38  |
|       | COUNT II – NEGLIGENCE PER SE.....                                | 41  |
|       | COUNT III – BREACH OF IMPLIED CONTRACT.....                      | 44  |
|       | COUNT IV – NEGLIGENT MISREPRESENTATION .....                     | 45  |
|       | COUNT V – UNJUST ENRICHMENT .....                                | 46  |
|       | COUNT VI – STATE CONSUMER PROTECTION LAWS.....                   | 47  |
|       | COUNT VII – STATE DATA BREACH STATUTES .....                     | 108 |
| VII.  | PRAYER FOR RELIEF .....  | 126 |
| VIII. | DEMAND FOR JURY TRIAL .....                                      | 127 |

Plaintiffs, identified below (collectively “Plaintiffs”), individually and on behalf of the Classes defined below of similarly situated persons, file this Second Consolidated Class Action Complaint. Plaintiffs file suit against Sonic Corp. and its affiliates and subsidiaries identified below (collectively, “Sonic” or the “Sonic Defendants”):

**I. INTRODUCTION**

1. In 2017, Sonic experienced a data security breach that compromised payment card data (“PCD”) from millions of transactions at hundreds of its stores. As a result, the PCD of millions of Sonic customers was at risk of being misused by criminals. (Hereafter referred to as the “Sonic Data Breach”).

2. Despite the fact that it was storing sensitive personal information that it knew was valuable to, and vulnerable to, cyber attackers, the Sonic Defendants were negligent in protecting their customers’ information, failing to take even the most basic security precautions that could have prevented cyber attackers from accessing customers’ data. Instead, Sonic used dated (*i.e.* old or out-of-date) or grossly inadequate computer systems and data security practices that allowed the hackers to easily access and take the customers’ personal data. Stealing this much data takes time, and there were numerous steps along the way when any company following current, standard IT security practices would or should have foiled the hackers. But, Sonic was negligent and failed to take these basic precautions.

3. At each of its Drive-In locations, Sonic displays the logo of the major card brands – Visa, Mastercard, American Express, Discover – that it accepts. Customers relied on such signs in choosing to shop Sonic and to pay for their purchases with a payment card with the understanding that Sonic followed reasonable, industry standard practices for the protection of the transaction and their PCD.

4. Sonic was negligent and failed to implement current, basic industry-accepted data security tools to prevent cyber attackers from accessing the cardholder data environment (“CDE”) in multiple ways, including:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Sonic also failed to utilize point-to-point encryption on all POS terminals. If Sonic had not been negligent and taken even one of these basic security steps, the cyber attackers would not have been able to access or use customers’ PCD or would have been detected at a much earlier date, reducing the number of customers whose PCD was compromised.

5. Any company with reasonable data security practices and procedures – especially a publicly-held company guarding valuable data that was a known target for cyber attackers –

would monitor for a data security breach. In other words, even if a company negligently left the “bank vault” open (as Sonic did), it would still have videos monitoring the bank vault, and alarms that would go off if intruders tried to leave with the loot. However, Sonic failed to implement (or turned off) many standard monitoring and alerting systems. The Sonic Defendants did have some monitoring systems turned on, and those systems sent out alerts when the cyber attackers entered various parts of their computer systems but Sonic either failed to review many of these alerts, or ignored the alerts altogether. As time went on, the cyber attackers were stealing so much data (*i.e.*, PCD) that basic information technology maintenance systems should have recognized and stopped the attack. Unfortunately, Sonic failed to properly implement or monitor those systems as well.

6. Sonic’s customers have been harmed by the Sonic Data Breach. For example, customers have had fraudulent charges made to their accounts, had fees charged to them, and lost use of their money for days or even weeks. Further, customers have had to spend time pouring over account statements to detect fraudulent charges, disputing fraudulent charges, and re-establishing accounts linked to a payment card that was compromised and cancelled as a result of the Sonic Data Breach. Additionally, the measures taken by the Sonic Defendants to date remain inadequate to protect Sonic’s customers from another data breach, posing a continued risk of additional, future harm to customers who pay with a payment card.

## **II. JURISDICTION AND VENUE**

7. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million exclusive of

interest and costs. At least one Plaintiff and one Defendant are citizens of different states. There are more than 100 putative class members.

8. This Court has personal jurisdiction over the Sonic Defendants because they regularly conduct business in Ohio and have sufficient minimum contacts in Ohio. Sonic has intentionally avail itself of this jurisdiction by marketing and selling products and services in Ohio.

9. Venue is proper in this Court pursuant to the United States Judicial Panel on Multidistrict Litigation's December 6, 2017 Transfer Order, MDL Case No. 2807, Dkt. No. 36.

### **III. THE PARTIES**

#### **A. PLAINTIFFS**

##### **Alabama**

10. Plaintiff Penny Bolin is a resident of Batesburg, Alabama. She is (and was during the period of the data breach) a citizen of the State of Alabama. She shopped at Sonic in West Columbia, South Carolina and Lexington, South Carolina several times in 2017 and paid with her debit card through one of Sonic's point-of-sale devices. In June 2017, after having shopped at Sonic, Ms. Bolin discovery unauthorized charges to the account linked to the debit card she had used at Sonic. She immediately notified her bank and disputed the charges. The Bank upon receiving the notification and dispute reversed the charges immediately, canceled her debit card and re-issued her debit card. Plaintiff Bolin was without the use of a debit card for about 2 days. Plaintiff Bolin spent 2 hours dealing with the bank and the consequences of the data breach. Plaintiff Bolin never received any individual notification from Sonic regarding the breach of the free credit monitoring offered by Sonic.

11. Plaintiff Carlton Donovan is a resident of Huntsville, Alabama. He is (and was during the period of the data breach) a citizen of the State of Alabama. He shopped at Sonic Drive-In locations in Madison, Alabama and Huntsville, Alabama in 2017 and paid with a debit card

through one of Sonic's point-of-sale devices. In mid-January 2018, after having shopped at Sonic, Plaintiff Donovan was notified of an unauthorized charge of \$79.24 by his bank which he immediately disputed. As a result of the dispute and unauthorized charge, Plaintiff's debit card was cancelled and he had to wait approximately 6 days for a new debit card. Once he received the new card he had to spend at least 3 hours changing the linked electronic billing accounts and electronic payment accounts to the new card. Plaintiff Donovan spent 6 hours dealing with the bank and the consequences of the data breach in addition to the deprivation of use of a debit card for his account for 6 days. Debit card cancelled and new one re-issued within a week. He never received any individual notification from Sonic regarding the breach or the free credit monitoring offered by Sonic.

### **Arizona**

12. Plaintiff Melvin Hildreth, III is a resident of Black Canyon, City, Arizona. He is (and was during the period of the data breach) a citizen of the State of Arizona. He shopped at a Sonic Drive-in location in Phoenix, AZ throughout 2017 and paid with a debit card through one of Sonic's point-of-sale devices. In September 2017, after he shopped at Sonic, he was notified by Mobile Alert that his debit card was being used without his permission. He immediately contacted the bank to cancel the card and got a new one re-issued. He also reviewed his August 2017 Checking Account statement and immediately disputed charges made on August 7, 2017 and August 8, 2017 totaling \$81.75. The Bank was able to process that dispute within 24 hours and those charges were reversed. Within 45 days, he was again notified via mobile alert that his replacement debit card was being used without his authorization. He immediately contacted the bank to cancel the card but instead of a new card being mailed to him, he had to take 4 hours off of work to travel to a branch location to meet with a Bank Manager to complete a questionnaire in

order for a new card to be issued. In December 2017, he was again notified via mobile alert that his second replacement debit card was being used without his authorization. He immediately contacted the bank to cancel the card and a new card was issued to him. Despite a new card being issued to him, Mr. Hildreth upon reviewing his January 2018 Checking Account statement again was forced to dispute two charges made on January 11, 2018 and January 16, 2018 respectively totaling \$100.60. The Bank was able to process that dispute and within 24 hours those charges were reversed. While the bank in each instance blocked the use of the card without his authorization, Mr. Hildreth spent approximately 7 hours dealing with the bank in all three instances to check his statements for other unauthorized activity and updating all accounts linked to each cancelled card breach or the free credit monitoring offered by Sonic. He never received any individual notification from Sonic regarding the breach or the free credit monitoring offered by Sonic.

13. Plaintiff Megan MacKay is a resident of Surprise, Arizona. She is (and was during the period of the data breach) a citizen of the State of Arizona. She shopped at various Sonic Drive-In locations in the Phoenix area in 2017 and paid with a debit card through one of Sonic's point-of-sale devices. On September 20, 2017, after having shopped at Sonic, Plaintiff MacKay's debit card information was used to make charges totaling \$69.29 without her permission, in Pasadena, California. These fraudulent charges depleted her bank account. Plaintiff MacKay disputed the fraudulent charges with her bank. After about three days, the bank refunded the fraudulent charges to her account. However, the inability to access and use her money in the interim caused some charges to be rejected causing Plaintiff MacKay embarrassment, stress and worry. Furthermore, as a result of being unable to access and use her funds while the fraud was being investigated by her bank, she had to charge purchases and bills to a credit card, which incurred credit card fees.



Plaintiff MacKay spent approximately ten (10) hours dealing with her bank to resolve the fraudulent charges, trying to trace back where the charge came from, and checking her credit and account statements for other fraudulent activity. Plaintiff MacKay continues to have to spend extra time reviewing her account statements for other fraudulent charges. She never received any individual notification from Sonic regarding the breach or the free credit monitoring offered by Sonic.

**Arkansas**

14. Plaintiff Paula Sbabo is a resident of Benton, Arkansas. She is (and was during the period of the data breach) a citizen of State of Arkansas. Paula Sbabo shopped at Sonic in Benton, Arkansas several times in 2017 and paid with a debit card through one of Sonic's point-of-sale devices. In March 2017, after having shopped at Sonic, Mrs. Sbabo discovered unauthorized charges to the account linked to the card Paula had at Sonic. Mrs. Sbabo immediately notified the bank, disputed the charges, and cancelled the debit card. She was able to get the unauthorized charges refunded but she did not order a new debit card for almost six (6) months due to her fear of other unauthorized charges. In December 2017, after having shopped at Sonic, Mrs. Sbabo was notified by her credit card company that her credit card was overdrawn as her Amazon Prime account had unilaterally changed the billing information from her cancelled debit card to her credit card. She was able to contact Amazon and her credit card company to get the charges reversed but spent almost 4 hours dealing with the data breach and these unauthorized charges. She never

received any individual notification from Sonic regarding the breach or the free credit monitoring offered by Sonic.

**California**

15. Plaintiff Henry Gil is a resident of San Diego, California. He is (and was during the period of the data breach) a citizen of the State of California. He shopped at the Sonic Drive-In in National City, California in 2017 and paid with a credit card through one of Sonic's point-of-sale devices. On or about October 1, 2017, after having shopped at Sonic, he was notified by his credit card company of several suspicious purchases, which he then disputed. By initiating the dispute, his credit card company cancelled his card and a new card was issued which took 3 to 4 weeks for him to receive. This credit card has a rewards program associated with it that Mr. Gil regularly took advantage of and was deprived of doing so in the time between the old card being cancelled and the new card being issued. During those 3 to 4 weeks the credit card company finished their investigation and reversed all of the charges, including all fees assessed. Plaintiff Gil spent approximately 3 hours dealing with his credit card company trying to resolve the charges, working with them to trace back where the charges came from and checking his account statements for other fraudulent activity. He continues to spend time reviewing his account statements and credit reports for other fraudulent charges. He never received any individual notification from Sonic regarding the breach or the free credit monitoring offered by Sonic.

**Indiana**

16. Plaintiff Shannon Gannon is a resident of South Bend, Indiana. She is (and was during the period of the data breach) a citizen of the State of Indiana. She shopped at Sonic in Mishawaka, Indiana and/or South Bend, Indiana approximately three times a week throughout 2017 and paid with her debit card through one of Sonic's point-of-sale devices. Beginning in

April 2017 after visiting Sonic, Plaintiff Gannon discovered ongoing unauthorized charges, of varying amounts, through self-monitoring of her account. Upon discovering the charges, she notified her bank, disputed the charges, and cancelled the debit card. In addition to initiating an internal review of the disputes made by Plaintiff Gannon, the Bank also terminated Plaintiff Gannon's existing online account user name and password which required Plaintiff Gannon to spend time to create a new online account password and then link that account to existing online bill pay accounts. Plaintiff Gannon spent weeks trying to get the unauthorized charges, which totaled at least \$1,000.00 reversed and was ultimately successful. However, she was without use of her funds during the two week period in which it took for the bank to finish its investigation. She has spent 40 hours, to date, monitoring her account for unauthorized charges and dealing with the bank to dispute the unauthorized charges. As of the date of the filing of this Complaint, she continues to monitor her account for unauthorized charges and anticipates the continued need to dispute more unauthorized charges with her bank as they may occur. Plaintiff Gannon never received any individual notification from Sonic regarding the breach or the free credit monitoring offered by Sonic.

### **Kentucky**

17. Plaintiff Shadawna Carson is a resident of Owensboro, Kentucky. She is (and was during the period of the data breach) a citizen of the State of Kentucky. She shopped at the Sonic Drive-In location in Owensboro, Kentucky on multiple occasions in 2017 and paid with a debit card through one of Sonic's point-of-sale devices. On or about February 20, 2017, after having shopped at Sonic, the Plaintiff was notified by her bank of unauthorized charges which resulted in an overdraft of her account totaling less than \$50.00 to the account linked to the debit card she used at Sonic. Her debit card was also cancelled and a new card was issued which required the

Plaintiff to spend time changing the linked e-pay accounts to that debit card to the new issued card. On or about June 30, 2017 after another Sonic visit, the Plaintiff was again notified by her bank of unauthorized charges which resulted in a second overdraft of her account totaling less than \$100.00 to the account linked to the debit card she used at Sonic. Her replacement debit card was also cancelled and a new card was issued which required the Plaintiff to spend time changing the linked e-pay accounts to that debit card to the new issued card. The Plaintiff spent over 60 hours working with her bank to review all of the unauthorized activity, disputing the charges, changing the linked e-pay accounts, and having to deal with the issues related to the 2 occurrences of unauthorized activity on the debit cards she used at Sonic. The bank did eventually reverse the charges but she was without the use of those funds for over 30 days. She never received any individual notification from Sonic regarding the breach or the free credit monitoring offered by Sonic.

### **Mississippi**

18. Plaintiff Septabeya Bean is a resident of Tupelo, Mississippi. She is (and was during the period of the data breach) a citizen of the State of Mississippi. Plaintiff Bean shopped at Sonic in Baldwin, Mississippi in 2017 and paid with a prepaid credit card linked to an account that her sister, Rosalind Johnson, opened for her use. Several times throughout 2017 after visiting Sonic, Plaintiff Bean noticed unauthorized charges had been made to the account. Each time she and/or her sister would have to spend time disputing the charges and trying to get the funds returned. Plaintiff Bean even had to miss work to try to get the unauthorized charges reversed and stopped. After hearing about the Sonic Data Breach, Plaintiff Bean reviewed her accounts and noticed that the charges appeared after her trips to Sonic and spoke to the manager of the Sonic she frequented but he was unwilling or unable to assist her. Eventually, because the unauthorized charges kept appearing on the account, it had to be closed. To date, Plaintiff Bean has spent

approximately 100 hours reviewing her account for fraudulent charges, trying to trace and stop the fraudulent charges, and dealing with the bank. In fact, dealing with the issues resulting from the data breach caused her to miss approximately 40 hours of work as bertrod operator where she earns \$10.20 per hour. As a result, Plaintiff Bean has suffered lost income of approximately \$408.00. Plaintiff Bean never received any individual notification from Sonic regarding the breach or the free credit monitoring offered by Sonic.

### **Nevada**

19. Plaintiff John Stephen Dolembro is a resident of Las Vegas, Nevada. He is (and was during the period of the data breach) a citizen of the State of Nevada. He shopped at Sonic Drive-In locations in the Las Vegas, Nevada area in 2017 and paid with his debit card through one of Sonic's point-of-sale devices. As a result of the data breach, Plaintiff Dolembro was at risk of imminent harm and decided to cancel his debit card to prevent criminals from being able to use the payment card data stolen in the Sonic data breach to access his financial accounts. He spent approximately one hour dealing with his financial institution to prevent fraud from the data breach. He was also inconvenienced by having to wait for a new card to arrive to access his account. Plaintiff Dolembro never received any individual notification from Sonic regarding the breach or the free credit monitoring offered by Sonic.

20. Plaintiff Linda Sipple is a resident of Pahrump, Nevada. She is (and was during the period of the data breach) a citizen of the State of Nevada. She shopped at the Sonic Drive-In location in Pahrump, Nevada in 2017 and paid with a debit card through one of Sonic's point-of-sale devices. On or about April 2, 2018, after having shopped at Sonic, Ms. Sipple was notified by her bank of NSF charges of \$8.00 related to two purchases on March 30, 2018 in the amount of \$259.78 and on April 2, 2018 of \$171.20. Ms. Sipple immediately reviewed her bank account

and disputed the March 30, 2018 and April 2, 2018 purchases. On April 4, 2018 the Bank completed their investigation and reversed all fees and charges which totaled \$430.99. Ms. Sipple had to spend four (4) hours of her time dealing with the bank, reviewing her statements, and disputing the charges. She never received any individual notification from Sonic regarding the breach or the free credit monitoring offered by Sonic.

### **New Mexico**

21. Plaintiffs Edward and Denise Ramirez are residents of Albuquerque, New Mexico. Mr. and Mrs. Ramirez are (and were during the period of the data breach) citizens of the State of New Mexico. They shopped at Sonic Drive-In locations in the Albuquerque area in 2017 and paid with a debit card through one of Sonic's point-of-sale devices. On April 3, 2017, after having shopped at Sonic, the Ramirez discovered that several unauthorized charges, totaling over \$1,000, were made to the account linked to the debit card that had been used at a Sonic Drive-In in Albuquerque earlier that same day. They contacted the bank to cancel the debit card. It took the bank approximately two weeks to investigate and return the funds. However, the lack of funds in the interim caused Mr. and Mrs. Ramirez's mortgage payment to bounce, which led to additional charges of \$36.50. Mr. and Mrs. Ramirez have spent, to date, approximately six (6) hours dealing with the bank to resolve the fraudulent charges, trying to trace where the charge came from, and checking their credit and account statements for other fraudulent activity. They never received any individual notification from Sonic regarding the breach or the free credit monitoring offered by Sonic.

### **North Carolina**

22. Plaintiff Vonda Hoover is a resident of Salisbury, North Carolina. She is (and was during the period of the data breach) a citizen of the State of North Carolina. She shopped at the

Sonic Drive-In location in Salisbury, North Carolina in 2017 and paid with a debit card through one of Sonic's point-of-sale devices. Shortly after shopping at Sonic she was contacted by her bank who notified her of attempted unauthorized use. The Bank immediately cancelled the card and reissued a new one. Plaintiff Hoover spent 3 hours having to deal with the data breach including reviewing her account to ensure no other unauthorized charges were attempted and going through to change all payment accounts issued to the linked card. She never received any individual notification from Sonic regarding the breach or the free credit monitoring offered by Sonic.

### **Ohio**

23. Plaintiff Cornelius Bogard is a resident of Cleveland, Ohio. He is (and was during the period of the data breach) a citizen of the State of Ohio. He shopped at Sonic Drive-In in Parma, Ohio, Streetsboro, Ohio, and Mayfield Heights, Ohio in 2017 and paid with a debit card through one of Sonic's point-of-sale devices. On or about November 4, 2017, after having shopped at Sonic, Plaintiff Bogard discovered fraudulent charges to his account totaling \$29.00. He immediately notified his bank, disputed the charges, and cancelled the debit card. Plaintiff Bogard has spent about seventy-two (72) hours addressing issues arising from the breach. In fact, dealing with the issues resulting from the data breach caused him to miss 20 hours of work as a plumber where he earns \$85 per hour. As a result, Plaintiff Bogard has suffered lost income in the amount of \$1,700.00. Plaintiff Bogard never received any individual notification from Sonic regarding the breach or the free credit monitoring offered by Sonic.

### **Pennsylvania**

24. Plaintiff Mark Korabelnikov is a resident of Pittsburgh, PA. He is (and was during the period of the data breach) a citizen of the State of Pennsylvania Plaintiff Korabelnikov shopped

at the Sonic location in Tarentum, PA in 2017 on multiple occasions. During at least one visit he paid with his debit card through one of Sonic's point-of-sale devices. During a second visit, he paid with a pre-paid American Express Debit Card through one of Sonic's point-of-sale devices. Following his visits, he was contacted by his bank by e-mail and telephone regarding unauthorized charges on his debit card which the Bank immediately reversed. To date Plaintiff Korabelnikov has spent over 6 hours reviewing his bank account for fraudulent charges, trying to trace and stop other fraudulent charges, dealing with the bank and also closing the pre-paid American Express card due to concerns with identity theft. Plaintiff Korabelnikov never received any individual notification from Sonic regarding the breach or the free credit monitoring offered by Sonic.

**Tennessee**

25. Plaintiff Patrick Blanford is a resident of Lafayette, Tennessee. He is (and was during the period of the data breach) a citizen of the State of Tennessee. He shopped at Sonic Drive-In locations in Carthage, Tennessee in 2017 and paid with a debit card through one of Sonic's point-of-sale devices. Following his trip to Sonic, he was notified that his debit card had been used, which caused his account to be overdrawn. Mr. Blanford is an over-the-road truck driver who had to miss four (4) driving days of work to stay home, travel back and forth to the bank branch in Hartsville, Tennessee, and work with the bank to review all unauthorized charges which cost him \$800.00 in his weekly salary. After the bank completed their investigation, they bank did not reverse the overdraft fee. He never received any individual notification from Sonic regarding the breach or the free credit monitoring offered by Sonic.

26. Plaintiff Cassandra Sharp is a resident of Memphis, Tennessee. She is (and was during the period of the data breach) a citizen of the State of Tennessee. She shopped at Sonic Drive-In locations in Memphis, Tennessee and Olive Branch, Mississippi, in 2017 and paid with



a credit card through one of Sonic's point-of-sale devices. On her October 2017 Account Statement, after having shopped at Sonic, Plaintiff Sharp received notification from her credit card company that her credit card had been compromised and that, as a result, the card was being cancelled and a new card was being issued. Plaintiff Sharp has spent 5 hours reviewing her account statements to determine whether any unauthorized charges had been made to her account. She never received any individual notification from Sonic regarding the breach or the free credit monitoring offered by Sonic.

### **Texas**

27. Plaintiff Esmeralda Hernandez is a resident of Houston, Texas. She is (and was during the period of the data breach) a citizen of the State of Texas. She shopped at Sonic Drive-In locations in Katy, Texas and the Houston area in 2017 and paid with a debit card through one of Sonic's point-of-sale devices. Between August 9, 2017 and October 25, 2017, after she had shopped at Sonic, thirteen (13) unauthorized purchases, totaling \$432.16, were made using Plaintiff Hernandez's debit card. Upon discovering these unauthorized charges, Plaintiff Hernandez disputed the charges with her bank. After the unauthorized charges were reported, the bank replaced Plaintiff Hernandez's debit card. She never received any individual notification from Sonic regarding the breach or the free credit monitoring offered by Sonic.

28. Plaintiff Barbara Kelley is a resident of Irving, Texas. She is (and was during the period of the data breach) a citizen of the State of Texas. She shopped at Sonic Drive-In locations in Irving, Texas in 2017 and paid with a debit card through one of Sonic's point-of-sale devices. Between July 1, 2017 and July 4, 2017, after having shopped at Sonic, fifteen (15) unauthorized charges of \$49.00 each were made to Plaintiff Kelley's debit card account, for a total of \$735.00 in unauthorized charges. These charges caused the account linked to Plaintiff Kelley's debit card

to become overdrawn and to incur \$102 in overdraft fees. Plaintiff Kelley immediately disputed the charges with her bank and they were conditionally reversed, pending investigation by her bank. Eventually, Ms. Kelley's bank determined that these charges were fraudulent and closed their investigation. After the unauthorized charges were reported, the bank replaced Plaintiff Kelley's debit card. She has spent between 1 and 3 hours dealing with the bank to dispute the charge and get her money returned, and updating all her accounts linked to the cancelled card and continues to spend time monitoring her checking account several times a week for additional fraudulent charges. She never received any individual notification from Sonic regarding the breach or the free credit monitoring offered by Sonic.

29. Plaintiff Dometric Pearson is a resident of Grand Prairie, Texas. She is (and was during the period of the data breach) a citizen of the State of Texas. She shopped at Sonic Drive-In locations in Grand Prairie, Texas in 2017 and paid with a credit card through one of Sonic's point-of-sale devices. On October 13, 2017, Plaintiff Pearson received an email notification from her bank that her credit card had been compromised in the Sonic Data Breach and that, as a result, the card was being cancelled and a new card was being issued. Plaintiff Pearson never received a replacement card and continues to be deprived of access to her credit and to spend time dealing with the bank to try to resolve issues resulting from her card being compromised in the data breach. In accordance with the Texas Deceptive Trade Practices Act-Consumer Protection Act V.T.C.A. Business and Commerce Code, Section 17.41, *et seq.*, Plaintiff Pearson, through counsel, sent a demand letter to Sonic on or about November 3, 2017. Sonic did not respond. She never received any individual notification from Sonic regarding the breach or the free credit monitoring offered by Sonic.

30. Plaintiff Angela Williams is a resident of Dallas, Texas. She is (and was during the period of the data breach) a citizen of the State of Texas. She shopped at Sonic Drive-In locations in the Dallas, Texas area in 2017, with the last visit being in early September 2017, and paid with a credit card through one of Sonic's point-of-sale devices. After her last visit to Sonic in September 2017, on or about October 14, 2017 while on an airplane traveling for a birthday celebration, Plaintiff Williams was notified by her credit card company of fraudulent activity on her credit card and the immediate cancelation of her card. The replacement credit card came 14 days later but during this time she was without the use of her credit card which made the entire birthday celebration weekend difficult as she had to borrow money from friends to pay for her hotel and incidentals. Following the two week investigation by her credit card company, all charges were reversed. In addition to the embarrassment, frustration, and humiliation of being deprived of her credit card during her vacation and having to rely on friends to borrow cash, Plaintiff Williams spent 4 hours with her credit card company reviewing the statements, tracing the charges, and ordering the replacement card. She never received any individual notification from Sonic regarding the breach or the free credit monitoring offered by Sonic.

#### **B. DEFENDANTS**

31. Defendant Sonic Corp. is a Delaware corporation with its headquarters and principal place of business in Oklahoma City, Oklahoma.

32. Sonic Industries Services, Inc. is an Oklahoma corporation with its headquarters and principal place of business in Oklahoma City, Oklahoma. It is a subsidiary of Sonic Corp.

33. Sonic Capital LLC is Delaware limited liability company with its headquarters and principal place of business in Oklahoma City, Oklahoma. It is a subsidiary of Sonic Industries Services, Inc.

34. Sonic Franchising LLC is a Delaware limited liability company with its headquarters and principal place of business in Oklahoma City, Oklahoma. Sonic Franchising LLC franchises restaurants. It is a subsidiary of Sonic Capital LLC.

35. Sonic Industries LLC is a Delaware limited liability company with its headquarters and principal place of business in Oklahoma City, Oklahoma. Sonic Industries, LLC is a franchise assets holder. It is a subsidiary of Sonic Capital LLC.

36. Sonic Restaurants, Inc. is an Oklahoma corporation with its headquarters and principal place of business in Oklahoma City, Oklahoma. Sonic Restaurants, Inc. operates restaurants. It is a subsidiary of Sonic Corp.

#### **IV. STATEMENT OF FACTS**

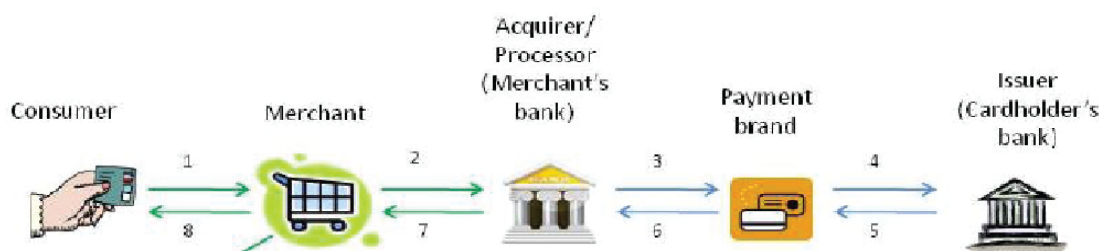
37. Sonic Corp., through its subsidiaries, operates and franchises the largest chain of drive-in restaurants (“Sonic Drive-Ins”) in the United States. For the fiscal year ended August 31, 2017, Sonic generated \$63.7 million in net income. *See* Sonic Corp. Annual Report (Form 10-K), (filed 10/27/2017 with SEC).

38. By sales, Sonic is the twelfth largest restaurant chain in America. <https://www.si.com/eats/2017/06/30/top-25-restaurant-chains-america-sales> (last visited 7/25/17). It is the fourth largest quick service burger restaurant chain. <https://www.qsrmagazine.com/reports/qsr50-2016-burger-segment-breakdown> (last visited 7/24/18).

39. When Sonic refers to “Sonic Corp.,” “Sonic,” “the Company,” “we,” “us” and “our” in its SEC filings and annual reports, it is referring to Sonic Corp. and its subsidiaries. *Id.* As of August 31, 2017, the Sonic system was comprised of 3,593 drive-ins, of which 6% were Company Drive-Ins and 94% were Franchise Drive-Ins. *Id.*

40. As set forth herein, all decisions relating to data security were made from Sonic's corporate headquarters in Oklahoma City, Oklahoma.

41. In a debit or credit card purchase transaction, card data must flow through multiple systems and parties to be processed. Generally, the cardholder presents a credit or debit card to a retailer to pay for merchandise. The card is then "swiped" and information about the card and the purchase is stored in the retailer's computers and then transmitted to the acquirer or processor (i.e., the retailer's bank). The acquirer relays the transaction information to the payment card company, who then sends the information to the issuer (i.e., cardholder's bank). The issuer then notifies the payment card company of its decision to authorize or reject the transaction. See graphic below:



|   |  |
|---|--|
| 1 | The consumer selects a card for payment. The cardholder data is entered into the merchant's payment system, which could be the point-of-sale (POS) terminal/software or an e-commerce website.   |
| 2 | The card data is sent to an acquirer/payment processor, whose job it is to route the data through the payments system for processing. With e-commerce transactions, a "gateway" provider may provide the link from the merchant's website to the acquirer. |
| 3 | The acquirer/processor sends the data to the payment brand (e.g. Visa, MasterCard, American Express, etc.) who forward it to the issuing bank/issuing bank processor   |
| 4 | The issuing bank/processor verifies that the card is legitimate, not reported lost or stolen, and that the account has the appropriate amount of credit/funds available to pay for the transaction.  |
| 5 | If so, the issuer generates an authorization number and routes this number back to the card brand. With the authorization, the issuing bank agrees to fund the purchase on the consumer's behalf.  |
| 6 | The card brand forwards the authorization code back to the acquirer/processor.   |
| 7 | The acquirer/processor sends the authorization code back to the merchant.  |
| 8 | The merchant concludes the sale with the customer.   |

Source: "Payments 101: Credit and Debit Card Payments," a white paper by First Data, at: <https://www.firstdata.com/downloads/thought-leadership/payments101wp.pdf>.

42. There are two points in the payment process where sensitive cardholder data is at risk of being exposed or stolen: pre-authorization when the merchant has captured a consumer's data and it is waiting to be sent to the acquirer; and post-authorization when cardholder data has been sent back to the merchant with the authorization response from the acquirer, and it is placed into some form of storage in the merchant's servers.

43. Encryption mitigates security weaknesses that exist when cardholder data has been stored, but not yet authorized, by using algorithmic schemes to transform plain text information into a non-readable format called "ciphertext." By scrambling the payment card data the moment it is swiped, hackers who steal the data are left with useless, unreadable text in the place of payment card numbers accompanying the cardholder's personal information.

44. Sonic Drive-In locations use one of several point-of-sale (POS) systems – [REDACTED], which are no longer supported and cannot be updated. Not all of these POS can and do provide end-to-end encryption.

45. On September 26, 2017, the cyber security blog, Krebs on Security, broke the news that a data breach at Sonic had exposed millions of credit and debit cards ("payment cards") used at Sonic and that the stolen information was being sold on "shadowy underground cybercrime stores." *See* "Breach at Sonic Drive-In may have impacted millions of credit, debit cards," Krebs on Security, 09/26/17, at <https://krebsonsecurity.com/2017/09/breach-at-sonic-drive-in-may-have-impacted-millions-of-credit-debit-cards/>. By the following day, the story had been picked up by major new outlets.

46. According to Sonic's public statements, it was made aware of "unusual activity" on payment cards used at Sonic by its payment card processor the week before. *See, e.g.* "Sonic

Drive-In hit by security breach” USA Today, 09/27/17, at <https://www.usatoday.com/story/tech/2017/09/27/sonic-drive-hit-security-breach/708850001/>.

47. Sonic delayed further and did not acknowledge that a data breach had occurred until October 4, 2017 and then only in statement on its corporate website. *See* “Sonic Drive-in: Notice of Payment Card Breach,” 10/04/17, at <http://ir.sonicdrivein.com/releasedetail.cfm?releaseid=1042818>. Even then, despite the fact that information on payment cards recently used at Sonic were being openly sold on the black market, Sonic only stated that “credit and debit card numbers *may* have been acquired without authorization.” *Id.* (emphasis added). Sonic also announced that it was making credit monitoring available to anyone who had shopped at any Sonic location at any time in 2017. *Id.*

48. Sonic has made no effort to notify the individuals whose data was stolen, leaving consumers to guess as to whether they are impacted and need to take measures to protect themselves from fraud. Indeed, for most customers, the first indication they had that they were impacted by the Sonic breach was seeing a fraudulent charge to their account.

49. More than five (5) months after news of the Sonic Data Breach had been broken, Sonic announced that the “investigations to date” had found “forensic evidence” that payment card data (“PCD”) was stolen from 314 Sonic Drive-In locations in 32 states. <https://www.sonicdrivein.com/-/notice-of-data-breach-faq>.

50. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Trustwave, the forensic investigator hired by Sonic at the request of the credit card brands, found [REDACTED]

A series of horizontal black bars of varying lengths, representing redacted text. The bars are arranged in a list-like fashion, with some bars being longer than others, suggesting different levels of redaction or different types of information being withheld. The bars are solid black and have sharp edges.

\_\_\_\_\_

\_\_\_\_\_



54. However, a customer cannot be confident that his data is secure even if he shopped at a Sonic Drive-In location using one of the other POS systems [REDACTED] approved by Sonic because many of the factors that the cyber attacker was able to exploit in the Sonic Data Breach – [REDACTED]

55. Customers who pay with a credit or debit card at Sonic continue to be at risk of having their PCD stolen and misused.

56. Despite warnings from its payment card processor, First Data<sup>1</sup>, and a number of high profile data breaches at other restaurant chains<sup>2</sup> in the years leading up to the Sonic Data Breach, which put Sonic on notice of the need to be vigilant against and take steps to prevent cyber attackers from stealing customers' data, Sonic's failed to take reasonable, industry-standard steps to secure its systems and its customers' data.

57. In fact, in the years leading up to the Sonic Data Breach, Sonic management received numerous warnings about vulnerabilities in its systems and processes that put customer data at risk. Still, Sonic continued to use old, out-of-date hardware and software that was unsupported and unsecure; Sonic failed to follow even basic security precautions, such as [REDACTED]. In fact, after news of the Sonic Data Breach broke, one person commented, anonymously:

---

<sup>1</sup> In a pamphlet, First Data warns: "*Data is extremely vulnerable and you are completely responsible for protecting it.*" "Payment Card Data Breaches: What You Need to Know About Your Risk and Liability," First Data Market Insight, at [https://www.firstdata.com/downloads/thought-leadership/13405\\_0714\\_Payment\\_Card\\_Data\\_Breach.pdf](https://www.firstdata.com/downloads/thought-leadership/13405_0714_Payment_Card_Data_Breach.pdf)

<sup>2</sup> See e.g. "7 Way to Protect Against a Data Breach," QSR Magazine, Feb. 2016, at <https://www.qsrmagazine.com/restaurant-software/7-ways-protect-against-data-breach>.

“Antiquated Software caused Breach... Executives too focused on delivering unnecessary shiny ‘new apps’ instead of fixing a problem they were all aware of, end result – millions of customers impacted...”

<https://www.thelayoff.com/sonic> (last visited 7/26/18).

58. Sonic, including its Board of Directors, were aware for years prior to the Sonic Data Breach that retailers, including restaurants like them, were prime targets for cyber attackers looking to steal valuable credit card data.

59. [REDACTED]

[REDACTED]

60. Despite the fact that Sonic knew retailers, like them, were targets of cyber attackers and the fact that [REDACTED]

[REDACTED], Sonic failed to devote sufficient resources to implement appropriate defensive measures or upgrades in a timely manner. As a result, cyber attackers were able to exploit the vulnerabilities in Sonic’s systems and steal the PCD of millions of Sonic customers.

61. Sonic customers across the United States have suffered real and imminent harm as a direct consequence of Sonic’s conduct, which includes (a) refusing to take adequate and reasonable measures to ensure its data systems were protected; (b) refusing to take available steps to prevent the breach from happening; (c) failing to disclose to its customers the material fact that

it did not have adequate computer systems and security practices to safeguard customers' personal and financial information; and (d) failing to provide timely and adequate notice of the data breach.

62. As a result of the data breach, the personal information, which included, but may not be limited to, payment card data ("PCD"), of 5 million Sonic customers has been exposed to criminals for misuse.

63. Remarkably, Sonic would not have even discovered the breach when it did except for its payment processor notifying it of "unusual activity" on payment cards after they had been used at Sonic and an Internet blog post by a data security watchdog that reported that massive batches of Sonic customers' payment cards have been offered for sale on online black markets to be purchased by criminals across the globe.

64. The injuries suffered by Plaintiffs and the proposed Classes as a direct result of the data breach include, *inter alia*:

- a. Unauthorized charges on their payment card accounts;
- b. Theft of their personal and financial information;
- c. Costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;
- d. Loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;
- e. Costs associated with time spent and the loss of productivity from taking time to address and attempting to ameliorate, mitigate, and deal with the actual and future

consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the data breach;

- f. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their personal information and PCD being placed in the hands of criminals and already misused via the sale of Plaintiffs' and Class members' information on the Internet black market;
- g. Damages to and diminution in value of their personal and financial information entrusted to Sonic for the sole purpose of making purchases at Sonic and with the mutual understanding that Sonic would safeguard Plaintiffs' and Class members' data against theft and not allow access to and misuse of their information by others;
- h. Money paid to Sonic stores during the period of the data breach in that Plaintiffs and Class members would not have gone to Sonic had Sonic disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' personal information and PCD and had Sonic provided timely and accurate notice of the data breach;
- i. Continued risk to their personal information and PCD, which remains in the possession of Sonic and which is subject to further breaches so long as Sonic continues to fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' data in its possession.

65. Examples of the harms to Sonic customers as a direct and foreseeable consequence of Sonic's conduct include the experiences of the representative Plaintiffs, which were described above.

66. Plaintiffs and Class Members would not have used their credit or debit cards to make purchases at Sonic—indeed, they would not have shopped at Sonic at all during the period of the data breach—had Sonic told them that it lacked adequate computer systems and data security practices to safeguard customers' personal and financial information from theft. Sonic also failed to provide Plaintiffs with timely and accurate notice of the data breach.

67. Plaintiffs and Class Members overpaid for the purchases they made at Sonic because an implied term of the contract was that Sonic would keep the transaction secure and Sonic failed to deliver a secure payment card transaction to Plaintiffs and the Class.

68. Plaintiffs and Class Members suffered actual injury from having his or her personal information and PCD compromised and/or stolen as a result of the data breach.

69. Plaintiffs and Class Members suffered actual injury and damages in paying money to and purchasing products from Sonic during the data breach that they would not have paid or purchased had Sonic disclosed that it lacked computer systems and data security practices adequate to safeguard customers' personal and financial information and had Sonic provided timely and accurate notice of the data breach.

70. Plaintiffs and Class Members suffered actual injury in the form of damages to and diminution in the value of his or her personal and financial identity information—a form of intangible property that each of the Plaintiffs entrusted to Sonic for the purpose of making purchases at Sonic and which was compromised in and as a result of the data breach.

71. Plaintiffs and Class Members suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by his or her personal and financial information being placed in the hands of criminals who have already misused such information stolen in the data breach via sale of Plaintiffs' and Class members' personal and financial information on the Internet black market.

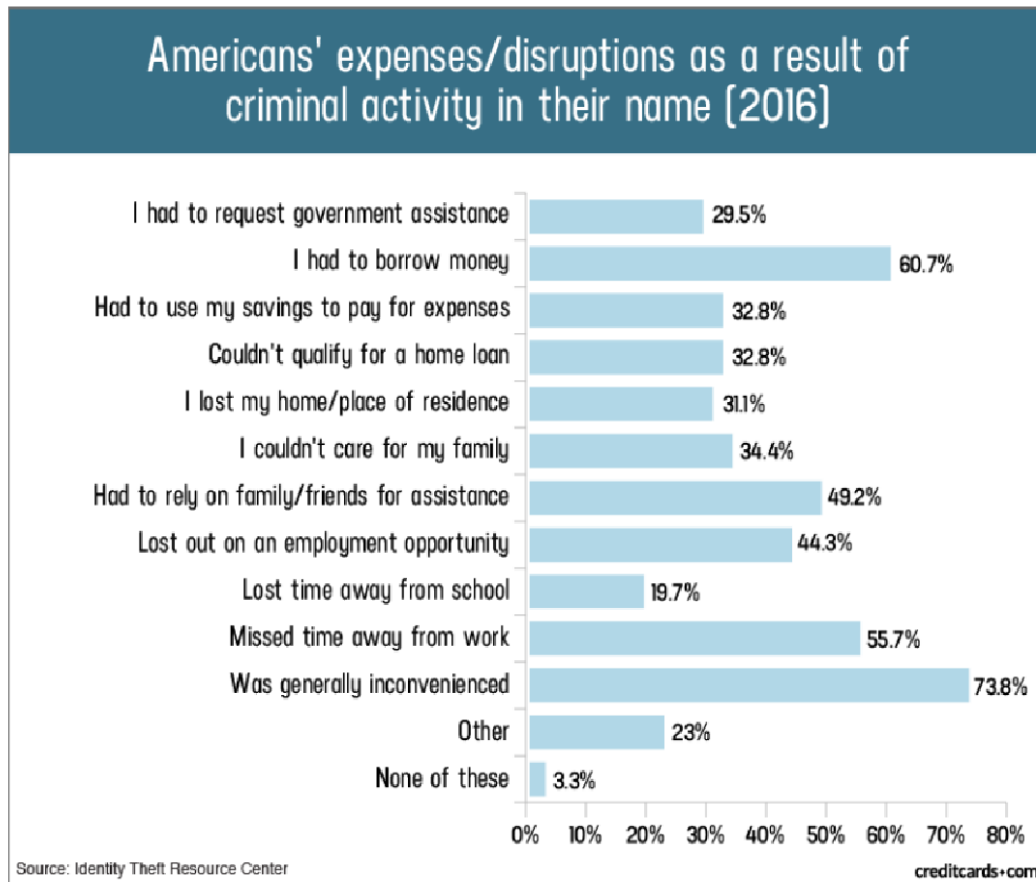
72. Plaintiffs and Class Members suffered actual injury in the form of time spent dealing with fraud resulting from the data breach and/or monitoring their accounts for fraud.

73. Plaintiffs and Class Members suffered actual injury in the form of fraudulent charges and the loss of use of funds while disputing such charges and, in some instances, additional damages resulting from such loss of use.

74. Plaintiffs have a continuing interest in ensuring that their private information, which remains in the possession of Sonic, is protected and safeguarded from future breaches.

75. None of the Plaintiffs who suffered a loss of use of their account funds, or who had restrictions placed on their accounts, as a result of the data breach was reimbursed for the loss of access to or restrictions placed upon their accounts and the resulting loss of use of their own funds.

76. A study by the Identity Theft Resource Center show the multitude of harms caused by fraudulent use of personal information:



Source: “Credit Card and ID Theft Statistics” by Jason Steele, 10/24/17, at: <https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php>. Plaintiffs and the Class have experienced one or more of these harms as a result of the data breach.

77. Sonic’s offer of credit monitoring to customer’s whose personal information was exposed is also inadequate because it does not continue long enough. There may be a time lag between when harm occurs versus when it is discovered, and also between when personal information or PCD is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit

identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

“Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown” by GAO, June 2007, at: <https://www.gao.gov/assets/270/262904.html>.

78. There is a strong probability that entire batches of stolen information have yet to be dumped on the black market, meaning Sonic customers could be at risk of fraud and identity theft for years into the future.

79. Plaintiffs and members of the classes defined below have or will suffer actual injury as a direct result of Sonic’s data breach. In addition to fraudulent charges and damage to their credit, many victims spent substantial time and expense relating to:

- a. Finding fraudulent charges;
- b. Canceling and reissuing cards;
- c. Purchasing credit monitoring and identity theft prevention;
- d. Addressing their inability to withdraw funds linked to compromised accounts;
- e. Removing withdrawal and purchase limits on compromised accounts;
- f. Taking trips to banks and waiting in line to obtain funds held in limited accounts;
- g. Spending time on the phone with or at the financial institution to dispute fraudulent charges;
- h. Resetting automatic billing instructions; and
- i. Paying late fees and declined payment fees imposed as a result of failed automatic payments.

80. As a direct and proximate result of Sonic’s conduct, Plaintiffs and the Class have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and



identity theft. Plaintiffs and Members of the Class now have to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing “freezes” and “alerts” with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come. Moreover, Plaintiffs and the Class have an interest in ensuring that their information, which remains in the possession of Sonic is protected from further breaches by the implementation of security measures and safeguards.

81. Plaintiffs and the Class have suffered, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

- a. Trespass, damage to and theft of their personal property including personal information and PCD;
- b. Improper disclosure of their personal information and PCD property;
- c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by customers’ personal information and PCD being placed in the hands of criminals and having been already misused via the sale of such information on the Internet black market;
- d. Damages flowing from Sonic’s untimely and inadequate notification of the data breach;
- e. Loss of privacy suffered as a result of the data breach;
- f. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach;

- g. Ascertainable losses in the form of deprivation of the value of customers' personal information for which there is a well-established and quantifiable national and international market; and
- h. The loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money customers were permitted to obtain from their accounts.

**V. CLASS ALLEGATIONS**

**A. NATIONWIDE CLASS**

82. Pursuant to Fed. R. Civ. P. 23(b)(1), (b)(2), (b)(3), and (c)(4), Plaintiffs assert common law claims for negligence (Count I), negligence per se (Count II), breach of implied contract (Count III), negligent misrepresentation (Count IV), deceit (Count V), unjust enrichment (Count VI), and injunctive / declaratory relief (Count IX), on behalf of nationwide class, defined as follows:

All persons who made a purchase at a Sonic Drive-In using a payment card during period January 1, 2017 through December 31, 2017 and whose personal information was vulnerable to compromise due to Sonic's failure to secure payment card data on its systems.

83. Excluded from the Classes are Defendants, any entity in which Defendants have a controlling interest, and Defendants' officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Classes is any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

**B. STATEWIDE CLASSES**

84. Alternatively, pursuant to Fed. R. Civ. P. 23(b)(1), (b)(2), (b)(3), and (c)(4), Plaintiffs assert common law claims for negligence (Count I), negligence per se (Count II), breach of implied contract (Count III), negligent misrepresentation (Count IV), deceit (Count V), unjust

enrichment (Count VI), and injunctive / declaratory relief (Count IX), on behalf of separate statewide classes for forty-five states (Alabama, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Virginia, Washington, West Virginia, Wisconsin, and Wyoming), defined as follows:

**Statewide [name of State] Class:** All residents of [name of State] who made a purchase at a Sonic Drive-In using a payment card during period January 1, 2017 through December 31, 2017 and whose personal information was vulnerable to compromise due to Sonic's failure to secure payment card data on its systems.

85. Excluded from the Classes are Defendants, any entity in which Defendants have a controlling interest, and Defendants' officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Classes is any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

86. Additionally, pursuant to Fed. R. Civ. P. 23(b)(1), (b)(2), (b)(3), and (c)(4), Plaintiffs assert statutory claims under state consumer protection statutes (Count VII) and state data breach notification statutes (Count VIII), on behalf of separate statewide classes for forty-five states (Alabama, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Virginia, Washington, West Virginia, Wisconsin, and Wyoming), defined as follows:

**Statewide [name of State] Class:** All residents of [name of State] who made a purchase at a Sonic Drive-In using a payment card during period January 1, 2017 through December 31, 2017 and whose personal information was vulnerable to compromise due to Sonic's failure to secure payment card data on its systems.

87. Excluded from the Classes are Defendants, any entity in which Defendants have a controlling interest, and Defendants' officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Classes is any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

**C. CERTIFICATION OF THE PROPOSED CLASSES IS APPROPRIATE**

88. Each of the proposed Classes meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

89. Numerosity: The PFI Report found evidence that over fourteen thousand (14,000) payment cards were stolen in the Sonic Data Breach but data necessary to more precisely determine the number of cards stolen no longer exists. However, just one batch of stolen payment cards sold on the dark web contained over five million cards. Therefore, it is reasonable to believe that millions of customers' payment card was compromised in the Sonic Data breach.

90. Commonality and Predominance: There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Classes, and those questions predominate over any questions that may affect individual members of the Classes. Common questions for the Classes include:

- a. Whether Defendants failed to adequately safeguard Plaintiffs' and the Classes' Personal Information;
- b. Whether Defendants failed to protect Plaintiffs' and the Classes' Personal Information;

- c. Whether Defendants' computer systems and data security practices used to protect Plaintiffs' and the Classes' Personal Information violated federal, state and local laws, or Defendants' duties;
- d. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiffs' and the Classes' Personal Information properly and/or as promised;
- e. Whether Defendants violated the consumer protection statutes and data breach notification statutes applicable to Plaintiffs and each of the Classes;
- f. Whether Defendants failed to notify Plaintiffs and members of the Classes about the Sonic Data Breach as soon as practical and without delay after the Sonic Data Breach was discovered;
- g. Whether Defendants acted negligently in failing to safeguard Plaintiffs' and the Classes' Personal Information;
- h. Whether Defendants entered into implied contracts with Plaintiffs and the members of the each of the Classes that included contract terms requiring Defendants to protect the confidentiality of Plaintiff's Personal Information and have reasonable security measures;
- i. Whether Defendants' conduct described herein constitutes a breach of their implied contracts with Plaintiffs and the members of each of the Classes;
- j. Whether Defendants should retain the money paid by Plaintiffs and members of each of the Classes to protect their Personal Information;
- k. Whether Plaintiffs and the members of the Classes are entitled to damages as a result of Defendants' wrongful conduct;

- l. Whether Plaintiffs and the members of the Classes are entitled to restitution as a result of Defendants' wrongful conduct;
- m. What equitable relief is appropriate to redress Defendants' wrongful conduct; and
- n. What injunctive relief is appropriate to redress the imminent and currently ongoing harm faced by members of the Classes.

91. **Typicality:** Plaintiffs' claims are typical of the claims of the members of the Classes. Plaintiffs and the members of the Classes sustained damages as a result of Defendants' uniform wrongful conduct during transactions with them.

92. **Adequacy:** Plaintiffs will fairly and adequately represent and protect the interests of the Classes, and have retained counsel competent and experienced in complex litigation and class actions. Plaintiffs have no interests antagonistic to those of the Classes, and there are no defenses unique to Plaintiffs. Plaintiffs and their counsel are committed to prosecuting this action vigorously on behalf of the members of the proposed Classes, and have the financial resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to those of the other members of the Classes.

93. **Risks of Prosecuting Separate Actions:** This case is appropriate for certification because prosecution of separate actions would risk either inconsistent adjudications which would establish incompatible standards of conduct for the Defendants or would be dispositive of the interests of members of the proposed Classes. Furthermore, the cardholder data environment still exists, and is still vulnerable to future attacks – one standard of conduct is needed to ensure the future safety of Sonic cardholder data environment.

94. **Policies Generally Applicable to the Classes:** This case is appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to

the Plaintiffs and proposed Classes as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct towards members of the Classes, and making final injunctive relief appropriate with respect to the proposed Classes as a whole. Defendants' practices challenged herein apply to and affect the members of the Classes uniformly, and Plaintiffs' challenge to those practices hinges on Defendants' conduct with respect to the proposed Classes as a whole, not on individual facts or law applicable only to Plaintiffs.

95. Superiority: This case is also appropriate for certification because class proceedings are superior to all other available means of fair and efficient adjudication of the claims of Plaintiffs and the members of the Classes. The injuries suffered by each individual member of the Classes are relatively small in comparison to the burden and expense of individual prosecution of the litigation necessitated by Defendants' conduct. Absent a class action, it would be virtually impossible for individual members of the Classes to obtain effective relief from Defendants. Even if members of the Classes could sustain individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties, including the Court, and would require duplicative consideration of the common legal and factual issues presented here. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court.

**VI. CAUSES OF ACTION**

**COUNT I – NEGLIGENCE**

**(Brought by the Nationwide Class or, alternatively, 44 Statewide Classes)**

96. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

97. Sonic solicited, gathered, and stored personal information, including PCD, of Plaintiffs and the Nationwide Negligence Class or, alternative, the Separate Statewide Negligence Classes (collectively, the “Class” as used in this Count) to facilitate sales transactions.

98. Sonic knew, or should have known, of the risks inherent in collecting and storing the personal information of Plaintiffs and the Class and the importance of adequate security. Sonic was well aware of the fact that hackers routinely attempted to access personal information, and PCD in particular, without authorization. Sonic also knew about numerous, well-publicized data breaches by other national retailer and restaurant chains.

99. Sonic owed duties of care to Plaintiffs and the Class whose personal information was entrusted to it. Sonic’s duties included the following:

- a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting personal information and PCD in its possession;
- b. To protect customers’ personal information and PCD using reasonable and adequate security procedures and systems that are compliant with the PCI-DSS standards and consistent with industry-standard practices;
- c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and
- d. To promptly notifying Plaintiffs and Class members of the data breach.



100. Because Sonic knew that a breach of its systems would potentially damage millions of its customers, including Plaintiffs and Class members, it had a duty to adequately protect their personal information.

101. Sonic owed a duty of care not to subject Plaintiffs and the Class to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

102. Sonic knew, or should have known, that its computer systems did not adequately safeguard the personal information of Plaintiffs and the Class.

103. Sonic breached its duties of care by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the personal information of Plaintiffs and the Class.

104. Sonic breached its duties of care by failing to provide prompt notice of the data breach to the persons whose personal information was compromised.

105. Sonic acted with reckless disregard for the security of the personal information of Plaintiffs and the Class because Sonic knew or should have known that its computer systems and data security practices were not adequate to safeguard the personal information that it collected and stored, which hackers were attempting to access.

106. Sonic acted with reckless disregard for the rights of Plaintiffs and the Class by failing to provide prompt and adequate notice of the data breach so that they could take measures to protect themselves from damages caused by the fraudulent use of the personal information compromised in the data breach.

107. Sonic had a special relationship with Plaintiffs and the Class. Plaintiffs' and the Class' willingness to entrust Sonic with their personal information was predicated on the

understanding that Sonic would take adequate security precautions. Moreover, only Sonic had the ability to protect its systems (and the personal information that it stored on them) from attack.

108. Sonic's own conduct also created a foreseeable risk of harm to Consumer Plaintiffs and Class members and their personal information. Sonic's misconduct included failing to:

- a. Secure its point-of-sale systems;
- b. Secure access to its servers;
- c. Comply with current, industry standard security practices;
- d. Follow the PCI-DSS standards;
- e. Encrypt PCD at the point-of-sale and during transit;
- f. Employ adequate network segmentation;
- g. Implement adequate system and event monitoring;
- h. Utilize up-to-date payment systems that provided more security against intrusion;
- i. Have anti-virus / anti-malware software running on all computers;
- j. Install updates and patches in a timely manner; and
- k. Implement the systems, policies, and procedures necessary to prevent this type of data breach.

109. Sonic also had independent duties under state laws that required it to reasonably safeguard Plaintiffs' and the Class' personal information and promptly notify them about the data breach.

110. Sonic breached the duties it owed to Consumer Plaintiffs and Class members in numerous ways, including:

- a. By creating a foreseeable risk of harm through the misconduct previously described;

- b. By failing to implement adequate security systems, protocols and practices sufficient to protect their personal information both before and after learning of the data breach;
- c. By failing to comply with the minimum industry data security standards, including the PCI-DSS, during the period of the data breach; and
- d. By failing to timely and accurately disclose that the personal information of Plaintiffs and the Class had been improperly acquired or accessed.

111. But for Sonic's wrongful and negligent breach of the duties it owed Plaintiffs and the Class members, their personal and financial information either would not have been compromised or they would have been able to prevent some or all of their damages.

112. As a direct and proximate result of Sonic's negligent conduct, Plaintiffs and the Class have suffered damages and are at imminent risk of further harm.

113. The injury and harm that Consumer Plaintiffs and Class members suffered (as alleged above) was reasonably foreseeable.

114. The injury and harm that Consumer Plaintiffs and Class members suffered (as alleged above) was the direct and proximate result of Sonic's negligent conduct.

115. Plaintiffs and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

## **COUNT II – NEGLIGENCE PER SE**

**(Brought by the Nationwide Class or, alternatively, 45 Statewide Classes)**

116. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

117. Pursuant to the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, Sonic had a duty to provide fair and adequate computer systems and data security to safeguard the

personal information, including PCD, of Plaintiffs and the Nationwide Negligence Class or, alternative, the Separate Statewide Negligence Per Se Classes (collectively, the “Class” as used in this Count).

118. The FTCA prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Sonic, of failing to use reasonable measures to protect personal information. The FTC publications and orders described above also formed part of the basis of Sonic’s duty in this regard.

119. Sonic solicited, gathered, and stored personal information, including PCD, of Plaintiffs and the Class to facilitate sales transactions which affect commerce.

120. Sonic violated the FTCA by failing to use reasonable measures to protect personal information of Plaintiffs and the Class and not complying with applicable industry standards, as described herein.

121. Sonic’s violation of the FTCA constitutes negligence *per se*.

122. Plaintiffs and the Class are within the class of persons that the FTCA was intended to protect.

123. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

124. As a direct and proximate result of Sonic’s negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, damages arising from their inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the data breach and/or false or fraudulent charges stemming from the data breach,

including but not limited to late fees charges; damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives including, *inter alia*, by contacting their financial institutions to place to dispute fraudulent charges, closing or modifying financial accounts, closely reviewing and monitoring their accounts for unauthorized activity which is certainly impending.

125. According to state laws in the following 12 states in which there are Sonic restaurants, Sonic had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Class Members' personal information:

- a. Arkansas: Ark. Code § 4-110-104;
- b. California: Cal Civ. Code § 1798.81.5;
- c. Connecticut: Conn. Gen. Stat. § 42-471;
- d. Florida: Fla. Stat. § 501.171(2);
- e. Indiana: Ind. Code § 24-4.9-3.5;
- f. Maryland: Md. Code. Comm. Law § 14-5303;
- g. Massachusetts: Mass. Gen Laws Ch. 93H, § 3(a);
- h. Nevada: Nev. Rev. Stat. § 603A.210;
- i. Oregon: Ore. Rev. Stat. § 646A.622(1);
- j. Rhode Island: R.I. Gen Laws § 11-49.2-2(2);
- k. Texas: Tex. Bus. & Com. Code § 521.052(a); and

1. Utah: Utah Code § 14-44-201(1)(a).

126. Sonic uses the same computer systems and security practices in all states in which there are Sonic restaurants.

127. Sonic breached its duties to Plaintiffs and the Class under these states' laws by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and the Class' personal information.

128. Sonic's violation of the FTCA and/or the state data security statutes listed in paragraph 125 constitutes negligence *per se*.

129. The injury and harm that Consumer Plaintiffs and Class members suffered (as alleged above) was the direct and proximate result of Sonic's negligence *per se*.

### **COUNT III – BREACH OF IMPLIED CONTRACT**

**(Brought by the Nationwide Class or, alternatively, 45 Statewide Classes)**

130. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

131. When Plaintiffs and the members of the Nationwide class or, alternatively, the members of the Separate Statewide Breach of Implied Contract Classes (collectively, the "Class" as used in this Count), provided their personal information to Sonic in making purchases at Sonic restaurants, they entered into implied contracts by which Sonic agreed to protect their personal information and timely notify them in the event of a data breach.

132. Sonic invited its customers, including Plaintiffs and the Class, to make purchases at Sonic restaurants using payment cards in order to increase sales by making purchases more convenient.

133. An implicit part of the offer was that Sonic would safeguard the personal information using reasonable or industry-standard means and would timely notify Plaintiffs' and the Class in the event of a data breach.

134. Sonic also implicitly and/or affirmatively represented that it collected and protected the personal information of Plaintiffs and the Class using “industry standard means.”

135. Based on the implicit understanding and also on Sonic’s representations (as described above), Plaintiffs and the Class accepted the offers and provided Sonic with their personal information by using their payment cards in connection with purchases at Sonic restaurants during the period of the data breach.

136. Plaintiffs and Class members would not have provided their personal information to Sonic had they known that Sonic would not safeguard their personal information as promised or provide timely notice of a data breach.

137. Plaintiffs and Class members fully performed their obligations under the implied contracts with Sonic.

138. Sonic breached the implied contracts by failing to safeguard Plaintiffs’ and Class members’ personal information and failing to provide them with timely and accurate notice when their personal information was compromised in the data breach.

139. The losses and damages Plaintiffs and Class members sustained (as described above) were the direct and proximate result of Sonic’s breach of the implied contract with Plaintiffs and Class members.

#### **COUNT IV – NEGLIGENT MISREPRESENTATION**

**(Brought by the Nationwide Class or, alternatively, 45 Statewide Classes)**

140. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

141. Sonic negligently and recklessly misrepresented material facts pertaining to the sale of food and drink to Plaintiffs and the Nationwide and Statewide Class Members by representing that they would maintain adequate data privacy and security practices and procedures to safeguard

Plaintiffs and Class Members' Personal Information from unauthorized disclosure, release, data breaches, and theft.

142. Sonic negligently and recklessly misrepresented material facts, pertaining to the sale of food and drink to Plaintiffs and Class Members by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiffs and Class Members' Personal Information.

143. Because of multiple warnings about the inadequacy of their data privacy and security practices, Sonic either knew or should have known that their representations were not true.

144. In reliance upon these misrepresentations, Plaintiffs and Class Members purchased food and drink from Sonic.

145. Had Plaintiffs and Class Members, as reasonable persons, known of Sonic's inadequate data privacy and security practices or that Sonic was failing to comply with the requirements of federal and state laws pertaining to the privacy and security of Class Members' Personal Information, they would not have purchased food and drink from Sonic and would not have entrusted Sonic with their Personal Information.

146. As a direct and proximate consequence of Sonic's negligent misrepresentations, Plaintiffs and Class Members have suffered the injuries alleged above.

#### **COUNT V – UNJUST ENRICHMENT**

**(Brought by the Nationwide Class or, alternatively, 45 Statewide Classes)**

147. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

148. Plaintiffs and members of the Nationwide class or, alternatively, the members of the Separate Statewide Unjust Enrichment Classes (collectively, the "Class" as used in this Count), conferred a monetary benefit on Sonic. Specifically, they made purchases from Sonic and provided Sonic with their personal information by using their payment cards for the purchases that



they would not have made if they had known that Sonic did not provide adequate protection of their personal information.

149. Sonic knew that Plaintiffs and the Class conferred a benefit on Sonic. Sonic profited from their purchases and used their personal information for its own business purposes.

150. Sonic failed to secure the Plaintiffs' and Class members' personal information, and, therefore, was unjustly enriched by the purchases made by Plaintiffs and the Class that they would not have made had they known that Sonic did not keep their personal information secure.

151. Plaintiffs and the Class have no adequate remedy at law.

152. Under the circumstances, it would be unjust for Sonic to be permitted to retain any of the benefits that Plaintiffs and Class members of the Class conferred on it.

153. Sonic should be compelled to disgorge into a common fund or constructive trust for the benefit of Plaintiffs and Class members proceeds that it unjustly received from them. In the alternative, Sonic should be compelled to refund the amounts that Plaintiffs and the Class overpaid.

## **COUNT VI – STATE CONSUMER PROTECTION LAWS**

**(Brought by the Statewide Classes Below)**

### **ARIZONA**

**Arizona Consumer Fraud Act, ARIZ. REV. STAT. §44-1521 *et seq.***

**(Brought by the Arizona Class)**

154. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

155. The Sonic Defendants operating in Arizona engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts in connection with the sale and advertisement of “merchandise” (as defined in the Arizona Consumer Fraud Act, ARIZ. REV. STAT. §44-1521(5)) in violation of ARIZ. REV. STAT. §44-1522(A), including but not limited to the following:

- a. Sonic misrepresented material facts to the Arizona Class, in connection with the sale of food and drink by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Arizona Class Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;
- b. Sonic misrepresented material facts to the Arizona Class, in connection with sale of food and drink, by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Arizona Class Members' Personal Information;
- c. Sonic omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Arizona Class Members' Personal Information, with the intent that others rely on the omission, suppression, and concealment;
- d. Sonic engaged in unfair acts and practices, in connection with the sale of food and drink by failing to maintain the privacy and security of Arizona Class Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Sonic Data Breach. These unfair acts and practices violated duties imposed by laws including the 15 U.S.C. § 45 and ARIZ. REV. STAT. § 18-545.
- e. Sonic engaged in unfair acts and practices in connection with the sale of food and drink by failing to disclose the Sonic Data Breach to Arizona Class Members in a timely and accurate manner, in violation of ARIZ. REV. STAT. § 18-545.
- f. Sonic engaged in unfair acts and practices with respect to the sale of food and drink by failing to take proper action following the Sonic Data Breach to enact adequate

privacy and security measures and protect Arizona Class Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

156. The above unfair and deceptive practices and acts by the Sonic were unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

157. Sonic knew or should have known that their computer systems and data security practices were inadequate to safeguard Arizona Class Members' Personal Information and that risk of a data breach or theft was highly likely. Sonic's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Arizona Class.

158. As a direct and proximate result of Sonic's unlawful practices, Arizona Class Members suffered injury and/or damages.

159. Arizona Class Members seek relief under ARIZ. REV. STAT. § 4421, et. seq., including, but not limited to, compensatory damages, punitive damages, injunctive relief, and/or attorneys' fees and costs.

**CALIFORNIA**

**California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq*  
(Brought by the California Class)**

160. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

161. The Sonic Defendants operating in California have violated California Business and Professions Code §17200 *et seq.* by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair

competition” as defined in CAL. BUS. PROF. CODE §17200 with respect to the sale of food and drink to the California Class, including but not limited to the following:

- a. Sonic engaged in deceptive acts and practices with regard to the sale of food and drink to the California Class by representing and advertising that they would maintain adequate data privacy and security practices and procedures to safeguard California Class Members’ Personal Information from unauthorized disclosure, release, data breaches, and theft; and representing and advertising that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of California Class Members’ Personal Information.
- b. Sonic engaged in deceptive acts and practices with regard to the sale of food and drink to the California Class by omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for California Class Members’ Personal Information. At the time that California Class members were making purchases at Sonic with their payment cards, Sonic failed to disclose to California Class Members that the Sonic’s data security systems failed to meet legal and industry standards for the protection of their Personal Information. Plaintiffs would not have purchased from Sonic if they had known about Defendants’ substandard data security practices or would have paid less.
- c. Sonic engaged in unfair acts and practices with respect to the sale of food and drink to the California Class Members by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs’ and California Class Members’ Personal Information with knowledge that the information would not be adequately protected; and by storing Plaintiffs’ and

California Class Members' Personal Information in an unsecure electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and California Class Members. Sonic's practice was also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws like 15 U.S.C. § 45 and CAL. CIV. CODE § 1798.81.5. The harm these practices caused to Plaintiffs and the California Class Members outweighed their utility, if any.

- d. Sonic engaged in unfair acts and practices with respect to the sale of food and drink by failing to disclose the Sonic Data Breach to California Class Members in a timely and accurate manner, contrary to the duties imposed by CAL. CIV. CODE § 1798.82. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and California Class Members. The harm these practices caused to Plaintiffs and the California Class Members outweighed their utility, if any.
- e. Sonic engaged in unfair acts and practices with respect to the sale of food and drink by failing to take proper action following the Sonic Data Breach to enact adequate privacy and security measures and protect California Class Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and California Class

Members. The harm these practices caused to Plaintiffs and the California Class Members outweighed their utility, if any.

- f. Sonic engaged in unlawful business practices by violating CAL. CIV. CODE § 1798.82.

162. As a direct and proximate result of Sonic's acts of unfair and unlawful practices and acts, the Plaintiffs were injured and lost money or property, including but not limited to the purchases they would not have otherwise made or overpayment for purchases, the loss of their legally protected interest in the confidentiality and privacy of their Personal Information, and additional losses described above.

163. Sonic knew or should have known that their computer systems and data security practices were inadequate to safeguard California Class Members' Personal Information and that the risk of a data breach or theft was highly likely. Defendants' actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the California Class.

164. California Class Members seek relief under CAL. BUS. & PROF. CODE § 17200, *et. seq.*, including, but not limited to, restitution to Plaintiffs and Class Members of money or property that the Defendants may have acquired by means of Defendants' deceptive, unlawful, and unfair business practices, restitutionary disgorgement of all profits accruing to Defendants because of their unlawful and unfair business practices, declaratory relief, attorney's fees and costs (pursuant to CAL. CODE CIV. PRO. §1021.5), and injunctive or other equitable relief.

**COLORADO**

**Colorado Consumer Protection Act, COLO. REV. STAT. §6-1-101 *et seq*  
(Brought by the Colorado Class)**

165. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

166. Colorado Class Members are actual or potential consumers of food and drink offered by Sonic.

167. Sonic engaged in deceptive, unfair, and unlawful trade acts or practices in the course of Sonic's business, vocation, or occupation, in violation of COLO. REV. STAT. §6-1-105, including but not limited to the following:

168. Sonic engaged in the above unfair or deceptive acts or practices in the course of their business.

169. As a direct and proximate result of Sonic's deceptive trade practices, Colorado Class Members suffered injuries to legally protected interests, including their legally protected interest in the confidentiality and privacy of their Personal Information.

170. The above unfair and deceptive practices and acts by Sonic were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

171. Sonic knew or should have known that their computer systems and data security practices were inadequate to safeguard Colorado Class Members' Personal Information and that risk of a data breach or theft was highly likely. Sonic actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Colorado Class.

172. Colorado Class Members seek relief under COLO. REV. STAT. § 6-1-101, et. seq., including, not limited to, compensatory damages, statutory damages, restitution, penalties, injunctive relief, and/or attorneys' fees and costs.

**CONNECTICUT**

**Connecticut Unfair Trade Practices Act, C.G.S. § 42-110a *et seq*  
(Brought by the Connecticut Class)**

173. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

174. Sonic engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of C.G.S. § 42-110b, including but not limited to the following:

- a. Sonic misrepresented and fraudulently advertised material facts pertaining to the sale of food and drink to the Connecticut Class by representing and advertising that they would maintain adequate data privacy and security practices and procedures to safeguard Connecticut Class Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;
- b. Sonic misrepresented material facts pertaining to the sale of food and drink to the Connecticut Class by representing and advertising that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Connecticut Class Members' Personal Information;
- c. Sonic omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Connecticut Class Members' Personal Information;
- d. Sonic engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Connecticut Class Members' Personal



Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Sonic Data Breach. These unfair acts and practices violated duties imposed by laws including the 15 U.S.C. § 45 and C.G.S. § 42-471.

- e. Sonic engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Sonic Data Breach to Connecticut Class Members in a timely and accurate manner, contrary to the duties imposed by C.G.S. § 36a-701b.
- f. Sonic engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the Sonic Data Breach to enact adequate privacy and security measures and protect Connecticut Class Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

175. As a direct and proximate result of Sonic deceptive trade practices, Connecticut Class Members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information.

176. The above unfair and deceptive practices and acts by Sonic were unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

177. Sonic knew or should have known that their computer systems and data security practices were inadequate to safeguard Connecticut Class Members' Personal Information and that risk of a data breach or theft was highly likely. Sonic's actions in engaging in the above-named

unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Connecticut Class.

178. Connecticut Class Members seek relief under C.G.S. § 42-110a *et seq.*, including, but not limited to, damages, statutory damages, restitution, penalties, injunctive relief, and/or attorneys' fees and costs.

**FLORIDA**  
**Deceptive and Unfair Trade Practices Act, FLA. STAT. § 501.201 *et seq***  
**(Brought by the Florida Class)**

179. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

180. At all times relevant herein, the members of the Florida Class were "consumers" within the meaning of the Florida Deceptive and Unfair Trade Practices Act, FLA. STAT. § 501.203.

181. The Sonic Defendants operating in Florida engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts in connection with the conduct of "trade or commerce" (as defined in the Florida Deceptive and Unfair Trade Practices Act, FLA. STAT. § 501.203), in violation of FLA. STAT. § 501.203, including but not limited to the following:

- a. Sonic misrepresented and fraudulently advertised material facts pertaining to the food and drink to the Florida Class by representing and advertising that they would maintain adequate data privacy and security practices and procedures to safeguard Florida Class Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;
- b. Sonic misrepresented material facts pertaining to food and drink to the Florida Class by representing and advertising that they did and would comply with the

requirements of relevant federal and state laws pertaining to the privacy and security of Florida Class Members' Personal Information;

- c. Sonic omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Florida Class Members' Personal Information;
- d. Sonic engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Florida Class Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Sonic Data Breach. These unfair acts and practices violated duties imposed by laws including the 15 U.S.C. § 45 and FLA. STAT. § 501.171.
- e. Sonic engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Sonic Data Breach to Connecticut Class Members in a timely and accurate manner, contrary to the duties imposed by FLA. STAT. § 501.171.
- f. Sonic engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the Sonic Data Breach to enact adequate privacy and security measures and protect Florida Class Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

182. As a direct and proximate result of Sonic's deceptive trade practices, Florida Class Members suffered an ascertainable loss of money or property, real or personal, as described above, including the payment for purchases they otherwise would not have made or overpayment for the purchases they did make and the loss of their legally protected interest in the confidentiality and privacy of their Personal Information.

183. The above unfair and deceptive practices and acts by Sonic were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

184. Sonic knew or should have known that their computer systems and data security practices were inadequate to safeguard Florida Class Members' Personal Information and that risk of a data breach or theft was highly likely. Sonic's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Florida Class.

185. Florida Class Members seek relief under FLA. STAT. § 501.201 *et seq.*, including, but not limited to, damages, statutory damages, restitution, penalties, injunctive relief, and/or attorneys' fees and costs pursuant to FLA. STAT. § 501.2105.

### **ILLINOIS**

#### **Illinois Consumer Fraud Act, 815 Ill. Comp. Stat. 505/1 *et seq* (Brought by the Illinois Class)**

186. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

187. Sonic engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of 815 Ill. Comp. Stat. § 505/2 and 815 Ill. Comp. Stat. § 530/20, including but not limited to the following:

- a. Sonic misrepresented and fraudulently advertised material facts pertaining to the sale of good and drink to the Illinois Class by representing and advertising that they would maintain adequate data privacy and security practices and procedures to safeguard Illinois Class Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;

- b. Sonic misrepresented material facts pertaining to the sale of food and drink to the Illinois Class by representing and advertising that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Illinois Class Members' Personal Information;
- c. Sonic omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Illinois Class Members' Personal Information with the intent that others rely on the omission, suppression, and concealment;
- d. Sonic engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Illinois Class Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Sonic Data Breach. These unfair acts and practices violated duties imposed by laws including 15 U.S.C. § 45 and 815 Ill. Comp. Stat. 510/2(a);
- e. Sonic engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Sonic Data Breach to Illinois Class Members in a timely and accurate manner, contrary to the duties imposed by 815 Ill. Comp. Stat. § 530/10(a);
- f. Sonic engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the Sonic Data Breach to enact adequate privacy and security measures and protect Illinois Class Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

188. As a direct and proximate result of Sonic deceptive trade practices, Illinois Class Members suffered injuries, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information, and damages, as described above.

189. The above unfair and deceptive practices and acts by Sonic were unethical, oppressive, and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

190. Sonic knew or should have known that their computer systems and data security practices were inadequate to safeguard Illinois Class Members' Personal Information and that risk of a data breach or theft was highly likely. Sonic's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Illinois Class.

191. Illinois Class Members seek relief under 815 Ill. Comp. Stat. 505/10a, including, but not limited to, damages, restitution, punitive damages, injunctive relief, and/or attorneys' fees and costs.

#### **ILLINOIS**

#### **Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. 505/2 *et seq* (Brought by the Illinois Class)**

192. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

193. While in the course of their businesses, Sonic engaged in deceptive trade practices by making false representations, including their representations that they had adequate computer systems and data security practices to protect Personal Information, when their computer systems and data security practices were inadequate, in violation of 815 Ill. Comp. Stat. 510/2(a)(5),(7).

194. Sonic knew or should have known that their computer systems and data security practices were inadequate and engaged in negligent, knowing, and/or willful acts of deception.

195. Illinois Class Members are likely to be damaged by the Defendants' deceptive trade practices.

196. Illinois Class Members seek relief under 815 Ill. Comp. Stat. 510, including, but not limited to, injunctive relief and attorney's fees.

**INDIANA**

**Indiana Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5-3  
(Brought by the Indiana Class Against Sonic)**

197. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

198. Members of the Indiana Class purchased food and drink from Sonic in Indiana for personal, family, and/or household purposes.

199. The Sonic Defendants are "suppliers" who engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of "consumer transactions" pertaining to the sale of food and drink in violation of Ind. Code § 24-5-0.5-3, including but not limited to the following:

200. As a direct and proximate result of Sonic deceptive trade practices, Indiana Class Members suffered injuries, including the costs of purchases they otherwise would not have made or overpayment for the purchases they did make as well as the loss of their legally protected interest in the confidentiality and privacy of their Personal Information, and damages.

201. The above unfair and deceptive practices and acts by Sonic were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

202. Sonic knew or should have known that their computer systems and data security practices were inadequate to safeguard Indiana Class Members' Personal Information and that risk of a data breach or theft was highly likely. Sonic's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Indiana Class.

203. Indiana Class Members seek relief under Ind. Code §24-5-0.5-4, including, not limited to damages, restitution, penalties, injunctive relief, and/or attorneys' fees and costs. Senior Members of the Indiana Class injured by Sonic unfair and deceptive trade practices also seek treble damages, pursuant to § Ind. Code §24-5-0.5-4(i).

**LOUISIANA**  
**Louisiana Unfair Trade Practices and Consumer Protection Law,**  
**La.Rev. Stat. § 54:1401 *et seq***  
**(Brought by the Louisiana Class)**

204. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

205. Sonic and the Louisiana Members are “persons” within the meaning of the La. Rev. Stat. Ann. § 51:1402(8).

206. The Louisiana Class Members are “consumers” within the meaning of La. Rev. Stat. Ann. § 51:1402(1).

207. Sonic engaged in “trade” or “commerce” within the meaning of La. Rev. Stat. Ann. § 51:1402(10).

208. The Louisiana Unfair Trade Practices and Consumer Protection Law (“Louisiana CPL”) makes unlawful “unfair or deceptive acts or practices in the conduct of any trade or commerce.” La. Rev. Stat. Ann. § 51:1405(A). Unfair acts are those that offend established public policy, while deceptive acts are practices that amount to fraud, deceit, or misrepresentation.

209. Sonic participated in unfair and deceptive acts and practices that violated the Louisiana CPL, including:

- a. Sonic misrepresented and fraudulently advertised material facts pertaining to the sale of good and drink to the Louisiana Class by representing and advertising that they would maintain adequate data privacy and security practices and procedures



to safeguard Louisiana Class Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;

- b. Sonic misrepresented material facts pertaining to the sale of food and drink to the Louisiana Class by representing and advertising that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Louisiana Class Members' Personal Information;
- c. Sonic omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Louisiana Class Members' Personal Information with the intent that others rely on the omission, suppression, and concealment;
- d. Sonic engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Louisiana Class Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Sonic Data Breach. These unfair acts and practices violated duties imposed by laws including 15 U.S.C. § 45 and La. Rev. Stat. Ann. § 51:3074(A) *et seq*;
- e. Sonic engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Sonic Data Breach to Louisiana Class Members in a timely and accurate manner, contrary to the duties imposed by La. Rev. Stat. Ann. § 51:3074(A) *et seq*;
- f. Sonic engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the Sonic Data Breach to enact adequate privacy

and security measures and protect Louisiana Class Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

210. Sonic's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Sonic's data security and ability to protect the confidentiality of consumers' Personal Information.

211. Sonic intended to mislead Louisiana Class Members and induce them to rely on its misrepresentations and omissions to purchase food and drink with a payment card.

212. Sonic's unfair and deceptive acts and practices were unethical, oppressive, and unscrupulous. These acts caused substantial injury to the Louisiana Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

213. Sonic acted intentionally, knowingly, and maliciously to violate the Louisiana CPL and recklessly disregarded the rights of the Louisiana Class Members. Sonic knew its security and privacy protections were inadequate.

214. Had Sonic disclosed to the Louisiana Class that its data systems were not secure and, thus, vulnerable to attack, Sonic would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law.

215. As a direct and proximate result of Sonic's unfair and deceptive acts and practices, the Louisiana Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

216. The Louisiana Class seeks all monetary and nonmonetary relief allowed by law, including actual damages; treble damages for Sonic's knowing violations of the Louisiana CPL; declaratory relief; attorneys' fees; and any other relief that is just and proper.

**MARYLAND**

**Maryland Consumer Protection Act, Md. Code Comm. Law, § 13-301 *et seq.*  
(Brought by the Maryland Class)**

217. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

218. Plaintiffs bring this claim against the Sonic Defendants operating in Maryland on behalf of the Maryland Class.

219. Maryland Class Members are "consumers" as meant by Md. Code Ann., Com. Law § 13-101.

220. Food and drink are "consumer goods" and/or "consumer services" as meant by Md. Code Ann., Com. Law § 13-101.

221. The unlawful trade practices, misrepresentations, and omissions described herein did not constitute "professional services" on the part of Sonic.

222. The Sonic Defendants operating in Maryland engaged in unlawful trade practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the "consumer goods" and/or "consumer services" in violation of Md. Code Ann., Com. Law § 13-301, including but not limited to the following:

- a. Sonic misrepresented material facts, pertaining to the sale of food and drink to the Maryland Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Maryland Class Members' Personal Information from unauthorized disclosure, release, data breaches, and

theft in violation of Md. Code Ann., Com. Law § 13-301(1), (2)(i), (2)(iv), (3), (5)(i), (9)(i), (9)(iii), and 14(xxi);

- b. Sonic misrepresented material facts, pertaining to the sale of food and drink to the Maryland Class by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Maryland Members' Personal Information in violation of Md. Code Ann., Com. Law § 13-301(1), (2)(i), (2)(iv), (3), (5)(i), (9)(i), (9)(iii), and 14(xxi);
- c. Sonic omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Maryland Class Members' Personal Information in violation of Md. Code Ann., Com. Law § 13-301(1), (2)(i), (2)(iv), (3), (5)(i), (9)(i), (9)(iii), and 14(xxi);
- d. Sonic engaged in unfair acts and practices with respect to the sale of food and drink by failing to maintain the privacy and security of Maryland Class Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Sonic Data Breach. These unfair acts and practices violated duties imposed by laws including the 15 U.S.C. § 45; Md. Code Regs. 31.16.08.01, et seq.); and Md. Code Ann. Com. Law § 14-3503;
- e. Sonic engaged in unfair acts and practices with respect to the sale of food and drink by failing to disclose the Sonic Data Breach to Maryland Class Members in a timely and accurate manner, in violation of Md. Code Com. Law § 14-3504(b)(3);
- f. Sonic engaged in unfair acts and practices with respect to the sale of food and drink by failing to take proper action following the Sonic Data Breach to enact adequate

privacy and security measures and protect Maryland Class Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

223. The above unfair and deceptive practices and acts by Sonic were unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

224. Sonic knew or should have known that their computer systems and data security practices were inadequate to safeguard Maryland Class Members' Personal Information and that risk of a data breach or theft was highly likely. Defendants' actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Maryland Class.

225. As a direct and proximate result of Sonic unlawful practices, Maryland Class Members suffered injury and/or damages.

226. Maryland Class Members seek relief under Md. Code Ann., Com. Law § 13-408, including, but not limited to, damages, injunctive relief, and attorneys' fees and costs.

**MICHIGAN**

**Michigan Consumer Protection Act, Mich. Comp. Laws § 445.901 *et seq*  
(Brought by the Michigan Class)**

227. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

228. Sonic engaged in unfair, unconscionable, or deceptive methods, acts, or practices in connection with the conduct of "trade or commerce" (as defined in the Michigan Consumer Protection Act, MICH. COMPILED LAWS ANN. § 445.902), in violation of MICH. COMPILED LAWS ANN. § 445.903, including but not limited to the following:

- a. Sonic misrepresented and fraudulently advertised material facts pertaining to the food and drink to the Michigan Class by representing and advertising that they would maintain adequate data privacy and security practices and procedures to safeguard Connecticut Class Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;
- b. Sonic misrepresented material facts pertaining to food and drink to the Michigan Class by representing and advertising that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Michigan Class Members' Personal Information;
- c. Sonic omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Michigan Class Members' Personal Information;
- d. Sonic engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Michigan Class Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Sonic Data Breach. These unfair acts and practices violated duties imposed by laws including the 15 U.S.C. § 45 and MICH. COMPILED LAWS ANN. § 445.72.
- e. Sonic engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Sonic Data Breach to Michigan Class Members in a timely and accurate manner, contrary to the duties imposed by MICH. COMPILED LAWS ANN. § 445.72.

- f. Sonic engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the Sonic Data Breach to enact adequate privacy and security measures and protect Michigan Class Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

229. As a direct and proximate result of Sonic deceptive trade practices, Michigan Class Members suffered an ascertainable loss of money or property, real or personal, as described above, including the payment for purchases they otherwise would not have made or overpayment for the purchases they did make and the loss of their legally protected interest in the confidentiality and privacy of their Personal Information.

230. The above unfair and deceptive practices and acts by Sonic were unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

231. Sonic knew or should have known that their computer systems and data security practices were inadequate to safeguard Michigan Class Members' Personal Information and that risk of a data breach or theft was highly likely. Sonic's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Michigan Class.

232. Michigan Class Members seek relief under MICH. COMPILED LAWS ANN. § 445.901 *et seq.*, including, but not limited to, damages, statutory damages, restitution, penalties, injunctive relief, and/or attorneys' fees and costs.

**MISSOURI**

**Missouri Merchandising Practices Act, Mo. Stat. § 407.010 *et seq.*  
(Brought by the Missouri Class)**

233. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

234. Plaintiffs bring this claim against the Sonic Defendants operating in Missouri on behalf of the Missouri Class.

235. Missouri Class Members purchased “merchandise” in “trade” or “commerce” as meant by Mo. Stat. § 407.010 when they purchased food and drink from Sonic for personal, family, and/or household purposes.

236. The Sonic Defendants operating in Missouri engaged in unlawful, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the services in violation of Mo. Stat. § 407.020(1), including but not limited to the following:

- a. Sonic misrepresented material facts, pertaining to the sale of food and drink to the Missouri Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Missouri Class Members’ Personal Information from unauthorized disclosure, release, data breaches, and theft;
- b. Sonic misrepresented material facts, pertaining to the sale of food and drink to the Missouri Class by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Missouri Class Members’ Personal Information;
- c. Sonic omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Missouri Class Members’ Personal Information;



- d. Sonic engaged in unfair acts and practices with respect to the sale of food and drink by failing to maintain the privacy and security of Missouri Class Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Sonic Data Breach. These unfair acts and practices violated duties imposed by laws including the 15 U.S.C. § 45; Missouri Statute § 375.936(4) and (6)(a); and Missouri Statute § 354-525;
- e. Sonic engaged in unlawful and deceptive acts and practices with respect to the sale of food and drink by failing to disclose the Sonic Data Breach to Missouri Class Members in a timely and accurate manner, in violation of Mo. Rev. Stat. § 407.1500(2)(1)(a);
- f. Sonic engaged in unlawful and deceptive acts and practices with respect to the sale of food and drink by failing to take proper action following the Sonic Data Breach to enact adequate privacy and security measures and protect Missouri Class Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

237. The above unlawful and deceptive acts and practices and acts by Sonic were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

238. Sonic knew or should have known that their computer systems and data security practices were inadequate to safeguard Missouri Class Members' Personal Information and that risk of a data breach or theft was highly likely. Sonic's actions in engaging in the above-named

unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Missouri Class.

239. As a direct and proximate result of Sonic unlawful practices, Missouri Class Members suffered an ascertainable loss of money or property, real or personal, as described above, including the purchases they otherwise would not have made or overpaying for the purchases they did make and the loss of their legally protected interest in the confidentiality and privacy of their Personal Information.

240. Missouri Class Members seek relief under Mo. Ann. Stat. § 407.025, including, but not limited to, injunctive relief, actual damages, punitive damages, and attorneys' fees and costs.

**NEBRASKA**

**Nebraska Consumer Protection Act, Neb. Rev. Stat. § 59-1601 *et seq.***

**(Brought by the Nebraska Class)**

241. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

242. Plaintiffs bring this claim against the Sonic Defendants operating in Nebraska on behalf of the Nebraska Class.

243. Sonic engaged in "trade and commerce," as meant by Neb. Rev. Stat. § 59-1601, by selling food and drink.

244. The Sonic Defendants operating in Nebraska engaged in unfair and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the services in violation of Neb. Rev. Stat. § 59-1602, including but not limited to the following:

- a. Sonic misrepresented material facts, pertaining to the sale of food and drink to the Nebraska Class by representing that they would maintain adequate data privacy and

security practices and procedures to safeguard Nebraska Class Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;

- b. Sonic misrepresented material facts, pertaining to the sale of food and drink to the Nebraska Class by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Nebraska Class Members' Personal Information;
- c. Sonic omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Nebraska Class Members' Personal Information;
- d. Sonic engaged in unfair acts and practices with respect to the sale of food and drink by failing to maintain the privacy and security of Nebraska Class Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Sonic Data Breach. These unfair acts and practices violated duties imposed by laws including the 15 U.S.C. § 45 and Neb. Rev. Stat. § 87-802;
- e. Sonic engaged in unlawful and deceptive acts and practices with respect to the sale of food and drink by failing to disclose the Sonic Data Breach to Nebraska Class Members in a timely and accurate manner, in violation of Neb. Rev. Stat. Ann. § 87-803(1);
- f. Sonic engaged in unlawful and deceptive acts and practices with respect to the sale of food and drink by failing to take proper action following the Sonic Data Breach to enact adequate privacy and security measures and protect Nebraska Class

Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

245. The above unlawful and deceptive acts and practices and acts by Sonic were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

246. Sonic knew or should have known that their computer systems and data security practices were inadequate to safeguard Nebraska Class Members' Personal Information and that risk of a data breach or theft was highly likely. Sonic's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Nebraska Class.

247. As a direct and proximate result of Sonic's unlawful practices, Nebraska Class Members suffered injury and/or damages.

248. Sonic Class Members seek relief under Neb. Rev. Stat. § 59-1609, including, but not limited to, injunctive relief, actual damages, and attorneys' fees and costs.

**NEBRASKA**

**Nebraska Uniform Deceptive Trade Practices Act, Neb. Rev. Stat. § 87-301 *et seq.***

**(Brought by the Nebraska Class)**

249. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

250. Plaintiffs bring this claim against the Sonic Defendants operating in Nebraska on behalf of the Nebraska Class.

251. The Sonic Defendants operating in Nebraska engaged in deceptive trade practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect

to the sale and advertisement of food and drink purchased by the Nebraska Class in violation of Neb. Rev. Stat. § 87-302, including but not limited to the following:

- a. Sonic misrepresented material facts, pertaining to the sale of food and drink to the Nebraska Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Nebraska Class Members' Personal Information from unauthorized disclosure, release, data breaches, and theft in violation of Neb. Rev. Stat. § 87-302(5), (7), (9), (14), and (15);
- b. Sonic misrepresented material facts, pertaining to the sale of food and drink to the Nebraska Class by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Nebraska Class Members' Personal Information in violation of Neb. Rev. Stat. § 87-302(5), (7), (9), (14), and (15);
- c. Sonic omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Nebraska Class Members' Personal Information in violation of Neb. Rev. Stat. § 87-302(5), (7), (9), (14), and (15);
- d. Sonic engaged in deceptive trade practices with respect to the sale of food and drink by failing to maintain the privacy and security of Nebraska Class Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Sonic Data Breach. These deceptive trade practices violated duties imposed by laws including 15 U.S.C. § 45 and Neb. Rev. Stat. Ann. § 87-803(1);

- e. Sonic engaged in deceptive trade practices with respect to the sale of food and drink by failing to disclose the Sonic Data Breach to Nebraska Class Members in a timely and accurate manner, in violation of Neb. Rev. Stat. Ann. § 87-803(1);
- f. Sonic engaged in deceptive trade practices with respect to the sale of food and drink by failing to take proper action following the Sonic Data Breach to enact adequate privacy and security measures and protect Nebraska Class Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

252. The above deceptive trade practices by Sonic were unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

253. Sonic knew or should have known that their computer systems and data security practices were inadequate to safeguard Nebraska Class Members' Personal Information and that risk of a data breach or theft was highly likely. Sonic's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Nebraska Class.

254. As a direct and proximate result of Sonic's unlawful practices, Nebraska Class Members suffered injury and/or damages.

255. Nebraska Class Members seek relief under Neb. Rev. Stat. § 87-303, including, but not limited to, injunctive relief, other equitable relief, and attorneys' fees and costs.

**NEVADA**

**Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. § 598.0915 *et seq.*  
(Brought by the Nevada Class)**

256. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

257. Plaintiffs bring this claim against the Sonic operating in Nevada on behalf of the Nevada Class.

258. In the course of their businesses, the Sonic Defendants operating in Nevada engaged in deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale of food and drink in violation of Nev. Rev. Stat. § 598.0915, including but not limited to the following:

- a. Sonic misrepresented material facts, pertaining to the sale of food and drink, to the Nevada Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Nevada Class Members' Personal Information from unauthorized disclosure, release, data breaches, and theft, in violation of Nev. Rev. Stat. § 598.0915(5), (7), (9), and (15);
- b. Sonic misrepresented material facts, pertaining to the sale of food and drink to the Nevada Class by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Nebraska Class Members' Personal Information, in violation of Nev. Rev. Stat. § 598.0915(5), (7), (9), and (15);
- c. Sonic omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Nevada Class Members' Personal Information, in violation of Nev. Rev. Stat. § 598.0915(5), (7), (9), and (15);

- d. Sonic engaged in deceptive trade practices with respect to the sale of food and drink by failing to maintain the privacy and security of Nevada Class Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Sonic Data Breach. These unfair acts and practices violated duties imposed by laws including the 15 U.S.C. § 45, Nev. Rev. Stat. § 695F.410, and Nev. Rev. Stat. Ann. § 603A.210;
- e. Sonic engaged in deceptive trade practices with respect to the sale of food and drink services by failing to disclose the Sonic Data Breach to Nevada Class Members in a timely and accurate manner, in violation of Nev. Rev. Stat. Ann. § 603A.220(1);
- f. Sonic engaged in deceptive trade practices with respect to the sale of food and drink by failing to take proper action following the Sonic Data Breach to enact adequate privacy and security measures and protect Nevada Class Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

259. The above unlawful and deceptive acts and practices and acts by Sonic were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

260. Sonic knew or should have known that their computer systems and data security practices were inadequate to safeguard Nevada Class Members' Personal Information and that risk of a data breach or theft was highly likely. Sonic's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Nevada Class.



261. As a direct and proximate result of Sonic's deceptive practices, Nevada Class Members suffered injury and/or damages.

262. Nevada Class Members seek relief under Nev. Rev. Stat. Ann. § 41.600, including, but not limited to, injunctive relief, other equitable relief, actual damages, and attorneys' fees and costs.

**NEW JERSEY**

**New Jersey Consumer Fraud Act, N.J. Stat. Ann., § 56:8-1 *et seq.*  
(Brought by the New Jersey Class)**

263. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

264. Plaintiffs bring this claim against the Sonic Defendants operating in New Jersey on behalf of the New Jersey Class.

265. The food and drink that Sonic sells is "merchandise" within the meaning of N.J. Stat. Ann. § 56:8-1. Sonic offers its merchandise to the public.

266. The Sonic Defendants operating in New Jersey engaged in unconscionable and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of food and drink in violation of N.J. Stat. Ann. § 56:8-2, including but not limited to the following:

- a. Sonic misrepresented material facts, pertaining to the sale of food and drink to the New Jersey Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard New Jersey Class Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;
- b. Sonic misrepresented material facts, pertaining to the sale of food and drink to the New Jersey Class by representing that they did and would comply with the

requirements of relevant federal and state laws pertaining to the privacy and security of New Jersey Class Members' Personal Information;

- c. Sonic knowingly omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for New Jersey Class Members' Personal Information with the intent that others rely on the omission, suppression, and concealment;
- d. Sonic engaged in unconscionable and deceptive acts and practices with respect to the sale of food and drink by failing to maintain the privacy and security of New Jersey Class Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Sonic Data Breach. These unfair acts and practices violated duties imposed by laws including 15 U.S.C. § 45 and N.J. Stat. Ann. § 56:8-163.
- e. Sonic engaged in unconscionable and deceptive acts and practices with respect to the sale of food and drink by failing to disclose the Sonic Data Breach to New Jersey Class Members in a timely and accurate manner, in violation of N.J. Stat. Ann. § 56:8-163(a);
- f. Sonic engaged in unconscionable and deceptive acts and practices with respect to the sale of food and drink by failing to take proper action following the Sonic Data Breach to enact adequate privacy and security measures and protect New Jersey Class Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

267. The above unlawful and deceptive acts and practices and acts Sonic were unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the

consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

268. Sonic knew or should have known that their computer systems and data security practices were inadequate to safeguard New Jersey Class Members' Personal Information and that risk of a data breach or theft was highly likely. Sonic's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the New Jersey Class.

269. As a direct and proximate result of Sonic's unconscionable or deceptive acts and practices, New Jersey Class Members suffered an ascertainable loss in moneys or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information.

270. New Jersey Class Members seek relief under N.J. Stat. Ann. § 56:8-19, including, but not limited to, injunctive relief, other equitable relief, actual damages, treble damages, and attorneys' fees and costs.

### **NEW MEXICO**

#### **New Mexico Unfair Practices Act, N.M. Stat. Ann. § 57-12-1 *et seq* (Brought by the New Mexico Class)**

271. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

272. Plaintiffs bring this claim against the Sonic Defendants operating in New Mexico on behalf of the New Mexico Class.

273. The Sonic Defendants operating in New Mexico engaged in unconscionable, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of food and drink in violation of N.M. Stat. Ann. § 57-12-3, including but not limited to the following:

- a. Sonic knowingly misrepresented material facts, pertaining to the sale of food and drink to the New Mexico Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard New Mexico Class Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;
- b. Sonic knowingly misrepresented material facts, pertaining to the sale of food and drink to the New Mexico Class by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of New Mexico Class Members' Personal Information;
- c. Sonic knowingly omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for New Mexico Class Members' Personal Information;
- d. Sonic engaged in unfair, unconscionable, and deceptive acts and practices with respect to the sale of food and drink by failing to maintain the privacy and security of New Mexico Class Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Sonic Data Breach. These unfair, unconscionable, and deceptive acts and practices violated duties imposed by laws including 15 U.S.C. § 45 and N.M. Admin. Code 13.1.3;
- e. Sonic engaged in unfair, unconscionable, and deceptive acts and practices with respect to the sale of food and drink by failing to disclose the Sonic Data Breach to New Mexico Class Members in a timely and accurate manner;

- f. Sonic engaged in unfair, unconscionable, and deceptive acts and practices with respect to the sale of food and drink by failing to take proper action following the Sonic Data Breach to enact adequate privacy and security measures and protect New Mexico Class Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

274. The above unfair, unconscionable, and deceptive acts and practices and acts by Sonic were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

275. Sonic knew or should have known that their computer systems and data security practices were inadequate to safeguard New Mexico Class Members' Personal Information and that risk of a data breach or theft was highly likely. Sonic's actions in engaging in the above-named unfair, unconscionable, and deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the New Mexico Class.

276. As a direct and proximate result of Sonic's unfair, unconscionable, and deceptive acts and practices, New Mexico Class Members suffered a loss in money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information.

277. New Mexico Class Members seek relief under N.M. Stat. Ann. § 57-12-10, including, but not limited to, injunctive relief, actual damages, and attorneys' fees and costs, as well as treble damages or \$300, whichever is greater, to the Plaintiffs.

**NEW YORK**

**New York General Business Law, N.Y. Gen. Bus. Law § 349 *et seq.*  
(Brought by the New York Class)**

278. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

279. Sonic engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a), including but not limited to the following:

- a. Sonic misrepresented and fraudulently advertised material facts, pertaining to the sale and/or furnishing food and drink to the New York Class by representing and advertising that they would maintain adequate data privacy and security practices and procedures to safeguard New York Class Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;
- b. Sonic misrepresented material facts, pertaining to sale and/or furnishing of food and drink to the New York Class by representing and advertising that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of New York Class Members' Personal Information;
- c. Sonic omitted, suppressed, and concealed the material fact of the inadequacy of their privacy and security protections for New York Class Members' Personal Information;
- d. Sonic engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of New York Class Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Sonic Data Breach. These unfair

acts and practices violated duties imposed by laws including the 15 U.S.C. § 45 and N.Y. Gen Bus. Law § 899-aa(2);

- e. Sonic engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Sonic Data Breach to New York Class Members in a timely and accurate manner, contrary to the duties imposed by N.Y. Gen Bus. Law § 899-aa(2);
- f. Sonic engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the Sonic Data Breach to enact adequate privacy and security measures and protect New York Class Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

280. As a direct and proximate result of Sonic's deceptive trade practices, New York Class Members suffered injury and/or damages, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information, and the loss of the benefit of their bargain.

281. The above unfair and deceptive practices and acts by Sonic were unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

282. Sonic knew or should have known that their computer systems and data security practices were inadequate to safeguard New York Class Members' Personal Information and that risk of a data breach or theft was highly likely. Sonic's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the New York Class.

283. Plaintiffs and New York Class Members seek relief under N.Y. Gen. Bus. Law § 349(h), including, but not limited to, actual damages, treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs.

**NORTH CAROLINA**

**North Carolina Unfair Trade Practices Act, N.C. Gen. Stat. Ann. § 75-1.1, *et. seq.*  
(Brought by the North Carolina Class)**

284. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

285. Plaintiffs bring this claim against Sonic on behalf of the North Carolina Class.

286. Sonic's sale, advertising, and marketing of food and drink affected commerce, as meant by N.C. Gen. Stat. § 75-1.1.

287. The Sonic Defendants operating in North Carolina engaged in unlawful, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of food and drink in violation of N.C. Gen. Stat. § 75-1.1, including but not limited to the following:

- a. Sonic misrepresented material facts, pertaining to the sale of food and drink to the North Carolina Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard North Carolina Class Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;
- b. Sonic misrepresented material facts, pertaining to the sale of food and drink to the North Carolina Class by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of North Carolina Class Members' Personal Information;



- c. Sonic omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for North Carolina Class Members' Personal Information;
- d. Sonic engaged in unfair, unlawful, and deceptive acts and practices with respect to the sale of food and drink by failing to maintain the privacy and security of North Carolina Class Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Sonic Data Breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including 15 U.S.C. § 45, N.C. Gen. Stat. § 58-39-1, et seq., and N.C. Gen. Stat. § 58-63-15(1) and (2);
- e. Sonic engaged in unfair, unlawful, and deceptive acts and practices with respect to the sale of food and drink by failing to disclose the Sonic Data Breach to North Carolina Class Members in a timely and accurate manner, in violation of N.C. Gen. Stat. Ann. § 76-65(a);
- f. Sonic engaged in unfair, unlawful, and deceptive acts and practices with respect to the sale of food and drink by failing to take proper action following the Sonic Data Breach to enact adequate privacy and security measures and protect North Carolina Class Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

288. The above unfair, unlawful, and deceptive acts and practices and acts by Sonic were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

289. Sonic knew or should have known that their computer systems and data security practices were inadequate to safeguard North Carolina Class Members' Personal Information and that risk of a data breach or theft was highly likely. Sonic's actions in engaging in the above-named unfair, unconscionable, and deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the North Carolina Class.

290. As a direct and proximate result of Sonic's unfair, unconscionable, and deceptive acts and practices, North Class Members suffered injury and/or damages.

291. North Carolina Class Members seek relief under N.C. Gen. Stat. §§ 75-16 and 75-16.1 including, but not limited to, injunctive relief, actual damages, treble damages, and attorneys' fees and costs.

#### **NORTH DAKOTA**

#### **North Dakota Unlawful Sales or Advertising Act, N.D. Cent. Code § 51-10-01 *et seq* (Brought by the North Dakota Class)**

292. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

293. Plaintiffs bring this claim against the Sonic Defendants operating in North Dakota on behalf of the North Dakota Class.

294. Sonic sells and advertises "merchandise," as meant by N.D. Cent. Code § 51-15-01, in the form of food and drink.

295. The Sonic Defendants operating in North Dakota engaged in deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with in connection to the sale and advertisement of food and drink in violation of N.D. Cent. Code § 51-15-01, including but not limited to the following:

- a. Sonic misrepresented material facts (intending for others to rely upon the misrepresentations), pertaining to the sale of food and drink to the North Dakota

Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard North Dakota Class Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;

- b. Sonic misrepresented material facts (intending for others to rely upon the misrepresentations), pertaining to the sale of food and drink to the North Dakota Class by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of North Dakota Class Members' Personal Information;
- c. Sonic omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for North Dakota Class Members' Personal Information, with the intent that others rely on the omission, suppression, and concealment;
- d. Sonic engaged in deceptive acts and practices with respect to the sale of food and drink by failing to maintain the privacy and security of North Dakota Class Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Sonic Data Breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including 15 U.S.C. § 45 and N.D. Admin. Code 45-14-01-01, et seq.
- e. Sonic engaged in deceptive acts and practices with respect to the sale of food and drink by failing to disclose the Sonic Data Breach to North Dakota Class Members in a timely and accurate manner, in violation of N.D. Cent. Code Ann. § 51-30-02;

- f. Sonic engaged in deceptive acts and practices with respect to the sale of food and drink by failing to take proper action following the Sonic Data Breach to enact adequate privacy and security measures and protect North Dakota Class Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

296. The above deceptive acts and practices and acts by Sonic were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

297. Sonic knew or should have known that their computer systems and data security practices were inadequate to safeguard North Dakota Class Members' Personal Information and that risk of a data breach or theft was highly likely. Sonic's actions in engaging in the above-named deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the North Dakota Class.

298. As a direct and proximate result of Sonic's deceptive acts and practices, Sonic acquired money or property from North Dakota Class Members.

299. North Dakota Class Members seek relief under N.D. Cent. Code Ann. § 51-15-09 including, but not limited to, injunctive relief, damages, restitution, treble damages, and attorneys' fees and costs.

**OKLAHOMA**

**Oklahoma Consumer Protection Act, Okla. Stat. Ann. tit. 15, § 751 *et seq.*  
(Brought by the Nationwide Class or the Oklahoma Class)**

300. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

301. Plaintiffs bring this claim against Sonic on behalf of the Oklahoma Class.

302. The Nationwide Class or, alternatively, Oklahoma Class Members purchased “merchandise,” as meant by Okla. Stat. tit. 15, § 752, in the form of food and drink.

303. The Nationwide Class or, alternatively, Oklahoma Class Members’ purchases of food and drink from Sonic constituted “consumer transactions” as meant by Okla. Stat. tit. 15, § 752.

304. Sonic engaged in unlawful, unfair, and deceptive trade practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale of the food and drink to the Nationwide Class or, alternatively, the Oklahoma Class in violation of Okla. Stat. tit. 15, § 753, including but not limited to the following:

- a. Sonic knowingly, or with reason to know, misrepresented material facts pertaining to the sale of food and drink to the Nationwide Class and/or the Oklahoma Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard the Nationwide Class Members’ and/or the Oklahoma Class Members’ Personal Information from unauthorized disclosure, release, data breaches, and theft in violation of Okla. Stat. tit. 15, § 753(5) and (8);
- b. Sonic knowingly, or with reason to know, misrepresented material facts pertaining to the sale of food and drink to the Nationwide Class and/or the Oklahoma Class by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the Nationwide Class Members’ and/or the Oklahoma Class Members’ Personal Information in violation of Okla. Stat. tit. 15, § 753(5) and (8);
- c. Sonic omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for the Nationwide Class Members’ and/or the

Oklahoma Class Members' Personal Information in violation of Okla. Stat. tit. 15, § 753(5) and (8);

- d. Sonic engaged in unfair, unlawful, and deceptive trade practices with respect to the sale of food and drink by failing to maintain the privacy and security of the Nationwide Class Members' and/or the Oklahoma Class Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Sonic Data Breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including 15 U.S.C. § 45 and Okla. Admin. Code §§ 365:35-1-40, 365:35-1-20;
- e. Sonic engaged in unlawful, unfair, and deceptive trade practices with respect to the sale of food and drink by failing to disclose the Sonic Data Breach to the Nationwide Class and/or the Oklahoma Class Members in a timely and accurate manner, in violation of 24 Okla. Sta. Ann. § 163(A);
- f. Sonic engaged in unlawful, unfair, and deceptive trade practices with respect to the sale of food and drink by failing to take proper action following the Sonic Data Breach to enact adequate privacy and security measures and protect the Nationwide Class Members' and/or the Oklahoma Class Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

305. The above unlawful, unfair, and deceptive trade practices and acts by Sonic were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

306. Sonic knew or should have known that their computer systems and data security practices were inadequate to safeguard the Personal Information of the Nationwide Class and/or Oklahoma Class and that risk of a data breach or theft was highly likely. Sonic's actions in engaging in the above-named deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Oklahoma Class.

307. As a direct and proximate result of Sonic deceptive acts and practices, the members of the Nationwide Class or, alternatively, the Oklahoma Class suffered injury and/or damages.

308. The Nationwide Class or, alternatively, the Oklahoma Class seeks relief under Okla. Stat. Ann. tit. 15, § 761.1 including, but not limited to, injunctive relief, actual damages, and attorneys' fees and costs.

### **OREGON**

#### **Oregon Unlawful Trade Practices Law, OR. REV. STAT. § 646.605 *et seq* (Brought by the Oregon Class)**

309. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

310. Sonic engaged in unlawful trade practices in the course of business (in violation of OR. REV. STAT. § 646.607, including but not limited to the following:

- a. Sonic misrepresented and fraudulently advertised material facts pertaining to the food and drink to the Oregon Class by representing and advertising that they would maintain adequate data privacy and security practices and procedures to safeguard Oregon Class Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;
- b. Sonic misrepresented material facts pertaining to food and drink to the Oregon Class by representing and advertising that they did and would comply with the

requirements of relevant federal and state laws pertaining to the privacy and security of Oregon Class Members' Personal Information;

- c. Sonic omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Oregon Class Members' Personal Information;
- d. Sonic engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Oregon Class Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Sonic Data Breach. These unfair acts and practices violated duties imposed by laws including the 15 U.S.C. § 45 and OR. REV. STAT. § 646A.600 *et seq.*
- e. Sonic engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Sonic Data Breach to Oregon Class Members in a timely and accurate manner, contrary to the duties imposed by OR. REV. STAT. § 646A.604.
- f. Sonic engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the Sonic Data Breach to enact adequate privacy and security measures and protect Oregon Class Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

311. As a direct and proximate result of Sonic deceptive trade practices, Oregon Class Members suffered an ascertainable loss of money or property, real or personal, as described above, including the payment for purchases they otherwise would not have made or overpayment for the purchases they did make and the loss of their legally protected interest in the confidentiality and privacy of their Personal Information.



312. The above unfair and deceptive practices and acts by Sonic were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

313. Sonic knew or should have known that their computer systems and data security practices were inadequate to safeguard Oregon Class Members' Personal Information and that risk of a data breach or theft was highly likely. Sonic's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Oregon Class.

314. Oregon Class Members seek relief under ORE. REV. STAT. ANN. § 646.638 including, but not limited to, damages, statutory damages, restitution, penalties, injunctive relief, and/or attorneys' fees and costs.

**PENNSYLVANIA**

**Pennsylvania Unfair Trade Practices Act, 73 Pa. Stat. Ann. § 201-1 *et seq.*  
(Brought by the Pennsylvania Class)**

315. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

316. Plaintiffs bring this claim against the Sonic Defendants operating in Pennsylvania on behalf of the Pennsylvania Class.

317. The Pennsylvania Class Members purchased food and/or drink from Sonic in "trade" and "commerce," as meant by 73 Pa. Cons. Stat. § 201-2, for personal, family, and/or household purposes.

318. The Sonic in Pennsylvania engaged in unlawful, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with

respect to the sale and advertisement of the services purchased by the Pennsylvania Class in violation of 73 Pa. Cons. Stat. Ann. § 201-3, including but not limited to the following:

- a. Sonic misrepresented material facts pertaining to the sale of food and drink to the Pennsylvania Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Pennsylvania Class Members' Personal Information from unauthorized disclosure, release, data breaches, and theft in violation of 73 Pa. Cons. Stat. Ann. § 201-3(4)(v), (ix), and (xxi);
- b. Sonic misrepresented material facts pertaining to the sale of food and drink to the Pennsylvania Class by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Pennsylvania Class Members' Personal Information in violation of 73 Pa. Cons. Stat. Ann. § 201-3(4)(v), (ix), and (xxi);
- c. Sonic omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Pennsylvania Class Members' Personal Information in violation of in violation of 73 Pa. Cons. Stat. Ann. § 201-3(4)(v), (ix), and (xxi);
- d. Sonic engaged in unfair, unlawful, and deceptive acts and practices with respect to the sale of food and drink by failing to maintain the privacy and security of Pennsylvania Class Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Sonic Data Breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including 15 U.S.C. § 45 and 40 Pa. Cons. Stat. Ann. § 1171.1(a)(1)(i) and (a)(2);

- e. Sonic engaged in unlawful, unfair, and deceptive acts and practices with respect to the sale of food and drink by failing to disclose the Sonic Data Breach to Pennsylvania Class Members in a timely and accurate manner, in violation of 73 Pa. Stat. § 2303(a);
- f. Sonic engaged in unlawful, unfair, and deceptive acts and practices with respect to the sale of food and drink by failing to take proper action following the Sonic Data Breach to enact adequate privacy and security measures and protect Pennsylvania Class Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

319. The above unlawful, unfair, and deceptive acts and practices by Sonic were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

320. Sonic knew or should have known that their computer systems and data security practices were inadequate to safeguard Pennsylvania Class Members' Personal Information and that risk of a data breach or theft was highly likely. Sonic's actions in engaging in the above-named deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Pennsylvania Class.

321. As a direct and proximate result of Sonic's deceptive acts and practices, the Pennsylvania Class Members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information.

322. Pennsylvania Class Members seek relief under 73 Pa. Cons. Stat. § 201-9.2, including, but not limited to, injunctive relief, actual damages or \$100 per Class Member, whichever is greater, treble damages, and attorneys' fees and costs.

**RHODE ISLAND**

**Rhode Island Deceptive Trade Practices Act, R.I. Gen. Laws § 6-13.1, *et. seq.*  
(Brought by the Rhode Island Class)**

323. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

324. Plaintiffs bring this claim against the Sonic Defendants operating in Rhode Island on behalf of the Rhode Island Class.

325. The Rhode Island Class Members purchased food and drink from Sonic in "trade" and "commerce," as meant by R.I. Gen. Laws § 6-13.1-1, for personal, family, and/or household purposes.

326. The Sonic Defendants operating in Rhode Island engaged in unlawful, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the goods purchased by the Rhode Island Class in violation of R.I. Gen. Laws Ann. § 6-13.1-2, including but not limited to the following:

327. The above unlawful, unfair, and deceptive acts and practices by Sonic were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

328. Sonic knew or should have known that their computer systems and data security practices were inadequate to safeguard Rhode Island Class Members' Personal Information and that risk of a data breach or theft was highly likely. Sonic's actions in engaging in the above-named

deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Rhode Island Class.

329. As a direct and proximate result of Sonic's deceptive acts and practices, the Rhode Island Class Members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information.

330. Rhode Island Class Members seek relief under R.I. Gen. Laws § 6-13.1-5.2, including, but not limited to, injunctive relief, other equitable relief, actual damages or \$200 per Class Member, whichever is greater, punitive damages, and attorneys' fees and costs.

**TENNESSEE**

**Tennessee Consumer Protection Act, Tenn. Code Ann. § 47-18-101 *et seq.***

**(Brought by the Tennessee Class)**

331. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

332. Plaintiffs bring this claim against the Sonic Defendants operating in Tennessee on behalf of the Tennessee Class.

333. Sonic advertised and sold "goods" or "services" in "trade" and "commerce," as meant by Tenn. Code § 47-18-103, in the form of food and drink.

334. The Sonic Defendants operating in Tennessee engaged in unlawful, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of food and drink in violation Tenn. Code § 47-18-104, including but not limited to the following:

- a. Sonic misrepresent material facts, pertaining to the sale of food and drink to the Tennessee Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Tennessee Class Members'

Personal Information from unauthorized disclosure, release, data breaches, and theft in violation of Tenn. Code § 47-18-104(b)(5) and (9);

- b. Sonic misrepresented material facts, pertaining to the sale of food and drink to the Tennessee Class by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Tennessee Class Members' Personal Information in violation of Tenn. Code § 47-18-104(b)(5) and (9);
- c. Sonic omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Tennessee Class Members' Personal Information in violation of Tenn. Code § 47-18-104(b)(5) and (9);
- d. Sonic engaged in unfair, unlawful, and deceptive acts and practices with respect to the sale of food and drink by failing to maintain the privacy and security of Tennessee Class Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Sonic Data Breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including 15 U.S.C. § 45 and Tenn. Code Ann. § 56-8-104(1)(A) and (2).
- e. Sonic engaged in unlawful, unfair, and deceptive acts and practices with respect to the sale of food and drink by failing to disclose the Sonic Data Breach to Tennessee Class Members in a timely and accurate manner, in violation of Tenn. Code. Ann. § 47-18-2107(b);
- f. Sonic engaged in unlawful, unfair, and deceptive acts and practices with respect to the sale of food and drink by failing to take proper action following the Sonic Data

Breach to enact adequate privacy and security measures and protect Tennessee Class Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

335. The above unlawful, unfair, and deceptive acts and practices by Sonic were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

336. Sonic knew or should have known that their computer systems and data security practices were inadequate to safeguard Tennessee Class Members' Personal Information and that risk of a data breach or theft was highly likely. Sonic's actions in engaging in the above-named deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Tennessee Class.

337. As a direct and proximate result of Sonic's deceptive acts and practices, the Tennessee Class Members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information.

338. Tennessee Class Members seek relief under Tenn. Code Ann. § 47-18-109, including, but not limited to, injunctive relief, actual damages, treble damages for each willful or knowing violation, and attorneys' fees and costs.

**TEXAS**

**Texas Deceptive Trade Practices and Consumer Protection Act,  
Tex. Bus. & Comm. Code § 17.41 *et seq.*  
(Brought by the Texas Class)**

339. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

340. Plaintiff Pearson, through counsel, sent a demand letter to Sonic on or about November 3, 2017.

341. Plaintiffs and Texas Class Members are consumers, as defined in TEX. BUS. & COM. CODE § 17.45(4), who purchased food and drink from Sonic.

342. Sonic engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Tex. Bus. & Com. Code § 17.46, including but not limited to the following:

- a. Sonic breached the implied warranty that payment card transactions would be kept secure in violation of Tex. Bus. & Comm. §17.50(a)(2) by failing to enact adequate privacy and security measures to protect Texas Class Members' Personal Information and not providing Texas Class Members with a secure transaction.
- b. Sonic engaged in unconscionable trade acts or practices in violation of Tex. Bus. & Com. §17.50(a)(3) by failing to maintain the privacy and security of Texas Class Members Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Sonic Data Breach. These unfair acts and practices violated duties imposed by laws including 15 U.S.C. § 45 and Tex. Bus. & Com. Code Ann. § 521.052(a).
- c. Sonic engaged in unconscionable trade acts or practices in violation of Tex. Bus. & Com. §17.50(a)(3) by failing to disclose the Sonic Data Breach to Texas Class



Members in a timely and accurate manner, contrary to the duties imposed by Tex. Bus. & Com. Code Ann. § 521.053(b);

- d. Sonic engaged in unconscionable trade acts or practices in violation of Tex. Bus. & Com. §17.50(a)(3) by failing to take proper action following the Sonic Data Breach to enact adequate privacy and security measures and protect Texas Class Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

343. As a direct and proximate result of Sonic's deceptive trade practices, Texas Class Members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information.

344. The above unfair and deceptive practices and acts by Sonic were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

345. Sonic knew or should have known that their computer systems and data security practices were inadequate to safeguard Texas Class Members' Personal Information and that risk of a data breach or theft was highly likely. Sonic's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Texas Class.

346. Texas Class Members seek relief under Tex. Bus. & Com. §17.50, including, but not limited to, economic damages, damages for mental anguish, treble damages, injunctive relief, restitution, and attorneys' fees and costs.

**WASHINGTON**

**Washington Consumer Protection Act, Wash. Rev. Code § 19.86.020 *et seq.*  
(Brought by the Washington Class)**

347. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

348. Sonic engaged in unfair, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code §19.86.020, including but not limited to the following:

- a. Sonic misrepresented and fraudulently advertised material facts pertaining to the food and drink to the Washington Class by representing and advertising that they would maintain adequate data privacy and security practices and procedures to safeguard Washington Class Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;
- b. Sonic misrepresented material facts pertaining to food and drink to the Washington Class by representing and advertising that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Washington Class Members' Personal Information;
- c. Sonic omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Washington Class Members' Personal Information;
- d. Sonic engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Washington Class Members Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Sonic Data Breach. These unfair

acts and practices violated duties imposed by laws including 15 U.S.C. § 45 and Wash. ADC 284-04-300.

- e. Sonic engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Sonic Data Breach to Washington Class Members in a timely and accurate manner, contrary to the duties imposed by § 19.255.010(1);
- f. Sonic engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the Sonic Data Breach to enact adequate privacy and security measures and protect Washington Class Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

349. As a direct and proximate result of Sonic's deceptive trade practices, Washington Class Members suffered injury and/or damages.

350. The above unfair and deceptive practices and acts by Sonic were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

351. Sonic knew or should have known that their computer systems and data security practices were inadequate to safeguard Washington Class Members' Personal Information and that risk of a data breach or theft was highly likely. Sonic's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Washington Class.

352. Washington Class Members seek relief under Wash. Rev. Code § 19.86.090, including, but not limited to, actual damages, treble damages, injunctive relief, and attorneys' fees and costs.

**WYOMING**

**Wyoming Consumer Protection Act, Wyo. Stat. Ann. § 40-12-101 *et seq*  
(Brought by the Wyoming Class)**

353. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

354. Sonic engaged in deceptive trade practices in the in the course of their business and in connection with a consumer transactions, in violation of Wyo. Stat. Ann. §40-12-105, including but not limited to the following:

- a. Sonic knowingly misrepresented and fraudulently advertised material facts pertaining to the food and drink to the Wyoming Class by representing and advertising that they would maintain adequate data privacy and security practices and procedures to safeguard Washington Class Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;
- b. Sonic knowingly misrepresented material facts pertaining to food and drink to the Wyoming Class by representing and advertising that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Wyoming Class Members' Personal Information;
- c. Sonic engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Wyoming Class Members Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Sonic Data Breach. These unfair acts and practices violated duties imposed by laws including 15 U.S.C. § 45 and Wyo. Stat. Ann. §40-12-502.

- d. Sonic engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Sonic Data Breach to Wyoming Class Members in a timely and accurate manner, contrary to the duties imposed by Wyo. Stat. Ann. §40-12-502;
- e. Sonic engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the Sonic Data Breach to enact adequate privacy and security measures and protect Wyoming Class Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

355. As a direct and proximate result of Sonic's deceptive trade practices, Wyoming Class Members suffered injury and/or damages.

356. The above unfair and deceptive practices and acts by Sonic were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

357. Sonic knew or should have known that their computer systems and data security practices were inadequate to safeguard Wyoming Class Members' Personal Information and that risk of a data breach or theft was highly likely. Sonic's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Wyoming Class.

358. Wyoming Class Members seek relief under Wyo. Stat. Ann. § 42-12-108, including, but not limited to, actual damages, treble damages, injunctive relief, and attorneys' fees and costs.

**COUNT VII – STATE DATA BREACH STATUTES**

**(Brought by the Statewide Classes Below)**

**CALIFORNIA**

**Cal. Civ. Code § 1798.80 *et seq*  
(Brought by the California Class)**

359. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

360. “[T]o ensure that personal information about California residents is protected,” the California legislature enacted Civil Code section 1798.81.5, which requires that any business that “owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.”

361. Sonic is a business that owns, maintains, and licenses “personal information,” within the meaning of 1798.81.5, about Plaintiffs and Class Members.

362. Sonic the violated Civil Code section 1798.81.5 by failing to implement reasonable measures to protect Class Members’ Personal Information.

363. Businesses that own or license computerized data that includes personal information, including account numbers, are required to notify California residents when their Personal Information has been acquired (or has reasonably believed to have been acquired) by unauthorized persons in a data security breach “in the most expedient time possible and without unreasonable delay.” Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include “the types of personal information that were or are reasonably believed to have been the subject of the breach.” Cal. Civ. Code § 1798.82.

364. The Sonic Defendants are businesses that own or license computerized data that includes personal information as defined by Cal. Civ. Code § 1798.82.

365. Plaintiffs and Class Members' Personal Information (e.g., credit or debit card numbers) includes personal information as covered by Cal. Civ. Code § 1798.82.

366. Because Sonic knew and/or had reasonable belief that Plaintiffs' Personal Information was acquired by unauthorized persons during the Sonic Data Breach, Sonic had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

367. By failing to disclose the Sonic Data Breach in a timely and accurate manner, Sonic violated Cal. Civ. Code § 1798.82.

368. As a direct and proximate result of Sonic's violations of the Cal. Civ. Code §§ 1798.81.5; 1798.82, Plaintiffs and Class Members suffered damages, as described above.

369. Plaintiffs and California Class Members seek relief under Cal. Civ. Code § 1798.84, including, but not limited to, actual damages and injunctive relief.

**COLORADO**  
**Colo. Rev. Stat. Ann. §6-1-716(2) *et seq.***  
**(Brought by the Colorado Class)**

370. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

371. The Sonic Defendants are required to accurately notify Plaintiffs and Class Members if they become aware of a breach of their data security system in the most expedient time possible and without unreasonable delay under Colo. Rev. Stat. Ann. § 6-1-716(2).

372. The Sonic Defendants are businesses that own or license computerized data that includes personal information as defined by Colo. Rev. Stat. Ann. § 6-1-716(1),(2).

373. Plaintiffs and Class Members' Personal Information (e.g., credit or debit card numbers) includes personal information as covered by Colo. Rev. Stat. Ann. § 6-1-716(1),(2).

374. Because the Sonic Defendants were aware of a breach of their security system, Sonic had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Colo. Rev. Stat. Ann. § 6-1-716 (2).

375. By failing to disclose the Sonic Data Breach in a timely and accurate manner, Sonic violated Colo. Rev. Stat. Ann. § 6-1-716 (2).

376. As a direct and proximate result of Sonic's violations of Colo. Rev. Stat. Ann. § 6-1-716(2), Plaintiffs and Class Members suffered damages, as described above.

377. Plaintiffs and Class Members seek relief under Colo. Rev. Stat. Ann. § 6-1-716(4), including, but not limited to, actual damages and equitable relief.

**GEORGIA**

**Ga. Code Ann. § 10-1-912(a) *et seq.*  
(Brought by the Georgia Class)**

378. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

379. The Sonic Defendants are required to accurately notify Plaintiffs and Class Members if they become aware of a breach of their data security system (that was reasonably likely to have caused unauthorized persons to acquire Plaintiffs and Class Members' Personal Information) in the most expedient time possible and without unreasonable delay under Ga. Code Ann. § 10-1-912(a).

380. The Sonic Defendants are businesses that own or license computerized data that includes personal information as defined by Ga. Code Ann. § 10-1-912(a).

381. Plaintiffs and Class Members' Personal Information (e.g., credit or debit card numbers) includes personal information as covered under Ga. Code Ann. § 10-1-912(a).



382. Because the Sonic Defendants were aware of a breach of their security system (that was reasonably likely to have caused unauthorized persons to acquire Plaintiffs and Class Members' Personal Information), Sonic had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Ga. Code Ann. § 10-1-912(a).

383. By failing to disclose the Sonic Data Breach in a timely and accurate manner, Sonic violated Ga. Code Ann. § 10-1-912(a).

384. As a direct and proximate result of Sonic's violations of Ga. Code Ann. § 10-1-912(a), Plaintiffs and Class Members suffered damages, as described above.

385. Plaintiffs and Class Members seek relief under Ga. Code Ann. § 10-1-912 including, but not limited to, actual damages and injunctive relief.

**IOWA**  
**Iowa Code Ann. § 715C.2(1) *et seq.***  
**(Brought by the Iowa Class)**

386. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

387. The Sonic Defendants are required to accurately notify Plaintiffs and Class Members if they become aware of a breach of their data security system in the most expeditious time possible and without unreasonable delay under Iowa Code Ann. § 715C.2(1).

388. The Sonic Defendants are businesses that own or license computerized data that includes personal information as defined by Iowa Code Ann. § 715C.2(1).

389. Plaintiffs and Class Members' Personal Information (e.g., credit and debit card numbers) includes personal information as covered under Iowa Code Ann. § 715C.2(1).

390. Because the Sonic Defendants were aware of a breach of their security system, Sonic had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Iowa Code Ann. § 715C.2(1).

391. By failing to disclose the Sonic Data Breach in a timely and accurate manner, Sonic violated Iowa Code Ann. § 715C.2(1).

392. As a direct and proximate result of Sonic's violations of Iowa Code Ann. § 715C.2(1), Plaintiffs and Class Members suffered damages, as above.

393. Plaintiffs and Class Members seek relief under Iowa Code Ann. § 714.16(7), including, but not limited to, actual damages and injunctive relief.

**KANSAS**

**Kan. Stat. Ann. § 50-7a02(a) *et seq.*  
(Brought by the Kansas Class)**

394. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

395. The Sonic Defendants are required to accurately notify Plaintiffs and Class Members if they become aware of a breach of their data security system (that was reasonably likely to have caused misuse of Plaintiffs and Class Members' Personal Information) in the most expedient time possible and without unreasonable delay under Kan. Stat. Ann. § 50-7a02(a).

396. The Sonic Defendants are businesses that own or license computerized data that includes personal information as defined by Kan. Stat. Ann. § 50-7a02(a).

397. Plaintiffs and Class Members' Personal Information (e.g., credit and debit card numbers) includes personal information as covered under Kan. Stat. Ann. § 50-7a02(a).

398. Because the Sonic Defendants were aware of a breach of their security system (that was reasonably likely to have caused misuse of Plaintiffs' and Class Members' Personal Information), Sonic had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Kan. Stat. Ann. § 50-7a02(a).

399. By failing to disclose the Sonic Data Breach in a timely and accurate manner, Sonic violated Kan. Stat. Ann. § 50-7a02(a).

400. As a direct and proximate result of Sonic's violations of Kan. Stat. Ann. § 50-7a02(a), Plaintiffs and Class Members suffered damages, as described above.

401. Plaintiffs and Class Members seek relief under Kan. Stat. Ann. § 50-7a02(g), including, but not limited to, broad equitable relief.

**KENTUCKY**

**Kentucky Computer Security Breach Notification Act, Ky. Rev. Stat. § 367.110 *et seq.*  
(Brought by the Kentucky Class)**

402. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

403. Sonic is required to accurately notify the Kentucky Class if it becomes aware of a breach of its data security system that was reasonably likely to have caused unauthorized persons to acquire Kentucky Class Members' Personal Information, in the most expedient time possible and without unreasonable delay under Ky. Rev. Stat. Ann. § 365.732(2).

404. Sonic is a business that holds computerized data that includes Personal Information as defined by Ky. Rev. Stat. Ann. § 365.732(2).

405. Kentucky Class Members' Personal Information includes Personal Information as covered under Ky. Rev. Stat. Ann. § 365.732(2).

406. Because Sonic was aware of a breach of its security system that was reasonably likely to have caused unauthorized persons to acquire Kentucky Class Members' Personal Information, Sonic had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Ky. Rev. Stat. Ann. § 365.732(2).

407. By failing to disclose the Sonic Data Breach in a timely and accurate manner, Sonic violated Ky. Rev. Stat. Ann. § 365.732(2).

408. As a direct and proximate result of Sonic's violations of Ky. Rev. Stat. Ann. § 365.732(2), the Kentucky Class Members have suffered damages, as described above.

409. The Kentucky Class seeks relief under Ky. Rev. Stat. Ann. § 446.070, including actual damages.

**LOUISIANA**  
**La. Rev. Stat. Ann. § 51:3074(A) *et seq.***  
**(Brought by the Louisiana Class)**

410. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

411. The Sonic Defendants are required to accurately notify Plaintiffs and Class Members if they become aware of a breach of their data security system (that was reasonably likely to have caused unauthorized persons to acquire Plaintiffs' and Class Members' Personal Information) in the most expedient time possible and without unreasonable delay under La. Rev. Stat. Ann. § 51:3074(C).

412. The Sonic Defendants are businesses that own or license computerized data that includes personal information as defined by La. Rev. Stat. Ann. § 51:3074(C).

413. Plaintiffs and Class Members' Personal Information (e.g., credit or debit card numbers) includes personal information as covered under La. Rev. Stat. Ann. § 51:3074(C).

414. Because the Sonic Defendants were aware of a breach of their security system (was reasonably likely to have caused unauthorized persons to acquire Plaintiffs' and Class Members' Personal Information), Sonic had an obligation to disclose the data breach in a timely and accurate fashion as mandated by La. Rev. Stat. Ann. § 51:3074(C).

415. As a direct and proximate result of Sonic's violations of La. Rev. Stat. Ann. § 51:3074(C), Plaintiffs and Class Members suffered damages, as described above.

416. Plaintiffs and Class Members seek relief under La. Rev. Stat. Ann. § 51:3075, including, but not limited to, actual damages.

**MARYLAND**

**Maryland Personal Information Protection Act, Md. Comm. Code § 14-3501 *et seq*  
(Brought by the Maryland Class)**

417. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

418. Under Md. Comm. Code § 14-3503(a), “[t]o protect Personal Information from unauthorized access, use, modification, or disclosure, a business that owns or licenses Personal Information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of Personal Information owned or licensed and the nature and size of the business and its operations.”

419. Sonic is a business that owns or licenses computerized data that includes Personal Information as defined by Md. Comm. Code §§ 14-3501(b)(1) and (2).

420. The Maryland Class Members are “individuals” and “customers” as defined and covered by Md. Comm. Code §§ 14-3502(a) and 14-3503.

421. The Maryland Class Members’ Personal Information includes Personal Information as covered under Md. Comm. Code § 14-3501(d).

422. Sonic did not maintain reasonable security procedures and practices appropriate to the nature of the Personal Information owned or licensed and the nature and size of its business and operations in violation of Md. Comm. Code § 14-3503.

423. The Sonic Data Breach was a “breach of the security of a system” as defined by Md. Comm. Code § 14-3504(1).

424. Under Md. Comm. Code § 14-3504(b)(1), “[a] business that owns or licenses computerized data that includes Personal Information of an individual residing in the State, when it discovers or is notified of a breach of the security system, shall conduct in good faith a reasonable

and prompt investigation to determine the likelihood that Personal Information of the individual has been or will be misused as a result of the breach.”

425. Under Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2), “[i]f, after the investigation is concluded, the business determines that misuse of the individual’s Personal Information has occurred or is reasonably likely to occur as a result of a breach of the security system, the business shall notify the individual of the breach” and that notification “shall be given as soon as reasonably practical after the business discovers or is notified of the breach of a security system.”

426. Because Sonic discovered a security breach and had notice of a security breach, Sonic had an obligation to disclose the Sonic Data Breach in a timely and accurate fashion as mandated by Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2).

427. By failing to disclose the Sonic Data Breach in a timely and accurate manner, Sonic violated Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2).

428. As a direct and proximate result of Sonic’s violations of Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2), the Maryland Class members suffered damages, as described above.

429. Pursuant to Md. Comm. Code § 14-3508, Sonic’s violations of Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2) are unfair or deceptive trade practices within the meaning of the Maryland Consumer Protection Act, 13 Md. Comm. Code §§ 13-101, *et seq.* and subject to the enforcement and penalty provisions contained within the Maryland Consumer Protection Act.

430. The Maryland Class Members seek relief under Md. Comm. Code §13-408, including actual damages and attorney’s fees.

**MICHIGAN**

**Mich. Comp. Laws Ann. § 445.72(1) *et seq*  
(Brought by the Michigan Class)**

431. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

432. The Sonic Defendants are required to accurately notify Plaintiffs and Class Members if they discover a security breach, or receive notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons), without unreasonable delay under Mich. Comp. Laws Ann. § 445.72(1).

433. The Sonic Defendants are businesses that own or license computerized data that includes personal information as defined by Mich. Comp. Laws Ann. § 445.72(1).

434. Plaintiffs and Class Members' Personal Information (e.g. credit and debit card numbers) includes personal information as covered under Mich. Comp. Laws Ann. § 445.72(1).

435. Because Sonic discovered a security breach and had notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons), Sonic had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Mich. Comp. Laws Ann. § 445.72(4).

436. As a direct and proximate result of Sonic's violations of Mich. Comp. Laws Ann. § 445.72(4), Plaintiffs and Class Members suffered damages, as above.

437. Plaintiffs and Class Members seek relief under Mich. Comp. Laws Ann. § 445.72(13), including, but not limited to, a civil fine.

**OREGON**

**Or. Rev. Stat. Ann. § 646A.604(1) *et seq.*  
(Brought by the Oregon Class)**

438. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

439. Pursuant to Or. Rev. Stat. Ann. § 646A.622(1), a business “that maintains records which contain personal information” of a Oregon resident “shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure.”

440. The Sonic Defendants are businesses that maintain records which contain personal information, within the meaning of Or. Rev. Stat. Ann. § 646A.622(1), about Plaintiffs and Class Members.

441. Sonic violated Or. Rev. Stat. Ann. § 646A.622(1) by failing to implement reasonable measures to protect Class Members’ Personal Information,

442. The Sonic Defendants are required to accurately notify Plaintiffs and Class Members if they become aware of a breach of their data security system in the most expeditious time possible and without unreasonable delay under Or. Rev. Stat. Ann. § 646A.604(1).

443. The Sonic Defendants are businesses that own, maintain, or otherwise possess data that includes consumers personal information as defined by Or. Rev. Stat. Ann. § 646A.604(1).

444. Plaintiffs and Class Members’ Personal Information (e.g., credit and debit card numbers) includes personal information as covered under Or. Rev. Stat. Ann. § 646A.604(1).

445. Because the Sonic Defendants discovered a breach of their security system, they had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Or. Rev. Stat. Ann. § 646A.604(1).



446. As a direct and proximate result of Sonic's violations of Or. Rev. Stat. Ann. §§ 646A.604(1) and 646A.622(1), Plaintiffs and Class Members suffered damages, as described above.

447. Plaintiffs and Class Members seek relief under Or. Rev. Stat. § 646A.624(3), including, but not limited to, actual damages and injunctive relief.

**SOUTH CAROLINA**  
**S.C. Code Ann. § 39-1-90(A) *et seq***  
**(Brought by the South Carolina Class)**

448. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

449. The Sonic Defendants are required to accurately notify Plaintiffs and Class Members following discovery or notification of a breach of their data security system (if personal information that was not rendered unusable through encryption, redaction, or other methods was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm) in the most expedient time possible and without unreasonable delay under S.C. Code Ann. § 39-1-90(A).

450. The Sonic Defendants are businesses that own or license computerized data or other data that includes personal identifying information as defined by S.C. Code Ann. § 39-1-90(A).

451. Plaintiffs and Class Members' Personal Information (e.g., credit and debit card numbers) includes personal identifying information as covered under S.C. Code Ann. § 39-1-90(D)(3).

452. Because Sonic discovered a breach of its data security system (in which personal information that was not rendered unusable through encryption, redaction, or other methods was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material

risk of harm), Sonic had an obligation to disclose the data breach in a timely and accurate fashion as mandated by S.C. Code Ann. § 39-1-90(A).

453. As a direct and proximate result of Sonic's violations of S.C. Code Ann. § 39-1-90(A), Plaintiffs and Class Members suffered damages, as described above.

454. Plaintiffs and Class Members seek relief under S.C. Code Ann. § 39-1-90(G), including, but not limited to, actual damages and injunctive relief.

**TENNESSEE**

**Tenn. Code Ann. § 47-18-2107(b) *et seq.*  
(Brought by the Tennessee Class)**

455. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

456. The Sonic are required to accurately notify Plaintiffs and Class Members following discovery or notification of a breach of their data security system (in which unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person) in the most expedient time possible and without unreasonable delay under Tenn. Code Ann. § 47-18-2107(b).

457. The Sonic Defendants are businesses that own or license computerized data that includes personal information as defined by Tenn. Code Ann. § 47-18-2107(a)(2).

458. Plaintiffs and Class Members' Personal Information (e.g., credit and debit card numbers) includes personal information as covered under Tenn. Code Ann. § 47-18-2107(a)(3)(A).

459. Because Sonic discovered a breach of their security system (in which unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person), Sonic had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Tenn. Code Ann. § 47-18-2107(b).

460. As a direct and proximate result of Sonic's violations of Tenn. Code Ann. § 47-18-2107(b), Plaintiffs and Class Members suffered damages, as described above.

461. Plaintiffs and Class Members seek relief under Tenn. Code Ann. §§ 47-18-2107(h), 47-18-2104(d), 47-18-2104(f), including, but not limited to, actual damages, injunctive relief and treble damages.

**VIRGINIA**

**Va. Code Ann. § 18.2-186.6(B) *et seq.*  
(Brought by the Virginia Class)**

462. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

463. The Sonic Defendants are required to accurately notify Plaintiffs and Class Members following discovery or notification of a breach of their data security system (if unencrypted or unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person who will, or it is reasonably believed who will, engage in identify theft or another fraud) without unreasonable delay under Va. Code Ann. § 18.2-186.6(B).

464. The Sonic Defendants are entities that own or license computerized data that includes personal information as defined by Va. Code Ann. § 18.2-186.6(B).

465. Plaintiffs and Class Members' Personal Information (e.g., credit and debit card numbers) includes personal information as covered under Va. Code Ann. § 18.2-186.6(A).

466. Because Sonic discovered a breach of their security system (in which unencrypted or unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person, who will, or it is reasonably believed who will, engage in identify theft or another fraud), Sonic had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Va. Code Ann. § 18.2-186.6(B).

467. As a direct and proximate result of Sonic's violations of Va. Code Ann. § 18.2-186.6(B), Plaintiffs and Class Members suffered damages, as described above.

468. Plaintiffs and Class Members seek relief under Va. Code Ann. § 18.2-186.6(I), including, but not limited to, actual damages.

**WASHINGTON**

**Wash. Rev. Code Ann. § 19.255.010(1) *et seq.*  
(Brought by Washington Class)**

469. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

470. The Sonic Defendants are required to accurately notify Plaintiffs and Class Members following discovery or notification of the breach of their data security system (if personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured) in the most expedient time possible and without unreasonable delay under Wash. Rev. Code Ann. § 19.255.010(1).

471. The Sonic Defendants are businesses that own or license computerized data that includes personal information as defined by Wash. Rev. Code Ann. § 19.255.010(1).

472. Plaintiffs and Class Members' Personal Information (e.g., credit and debit card numbers) includes personal information as covered under Wash. Rev. Code Ann. § 19.255.010(5).

473. Because Sonic discovered a breach of its security system (in which personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured), Sonic had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Wash. Rev. Code Ann. § 19.255.010(1).

474. As a direct and proximate result of Sonic's violations of Wash. Rev. Code Ann. § 19.255.010(1), Plaintiffs and Class Members suffered damages, as described above.

475. Plaintiffs and Class Members seek relief under Wash. Rev. Code Ann. §§ 19.255.010(10)(a), 19.255.010(10)(b) including, but not limited to, actual damages and injunctive relief.

**WYOMING**

**Wyo. Stat. Ann. § 40-12-502 *et seq.*  
(Brought by Wyoming Class)**

476. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

477. The Sonic Defendants are required to accurately notify Plaintiffs and Class Members when they become aware of a breach of its data security system (if the misuse of personal identifying information has occurred or is reasonably likely to occur) in the most expedient time possible and without unreasonable delay under Wyo. Stat. Ann. § 40-12-502(a).

478. The Sonic Defendants are businesses that own or license computerized data that includes personal information as defined by Wyo. Stat. Ann. § 40-12-502(a).

479. Plaintiffs and Class Members' Personal Information (e.g., credit and debit card numbers) includes personal information as covered under Wyo. Stat. Ann. § 40-12-502(a).

480. Because the Sonic Defendants were aware of a breach of their data security system (in which the misuse of personal identifying information has occurred or is reasonably likely to occur), Sonic had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Wyo. Stat. Ann. § 40-12-502(a).

481. As a direct and proximate result of Sonic's violations of Wyo. Stat. Ann. § 40-12-502(a), Plaintiffs and Class Members suffered damages, as described above.

482. Plaintiffs and Class Members seek relief under Wyo. Stat. Ann. § 40-12-502(f), including, but not limited to, actual damages and broad equitable relief.

**COUNT VIII – INJUNCTIVE / DECLARATORY RELIEF**  
**(Brought by Nationwide Class or, alternatively, 45 Statewide Classes)**

483. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

484. Plaintiffs and members of the Breach of Implied Contract classes entered into an implied contract that required Sonic to provide adequate security for the personal information it collected from their payment card transactions.

485. Sonic owes duties of care to Plaintiffs and the members of the Nationwide class or, alternatively, the separate statewide Negligence classes, that require it to adequately secure personal information.

486. Sonic still possesses personal information regarding the Plaintiffs' and the Class members.

487. Since the data breach, Sonic announced no changes to its data security to fix the vulnerabilities in its systems which permitted the intrusions and to prevent further attacks.

488. Accordingly, Sonic still has not satisfied its contractual obligations and legal duties to Plaintiffs and the Breach of Implied Contract and Negligence Classes. In fact, now that Sonic's lax approach towards information security has become public, the personal information in Sonic's possession is more vulnerable than previously.

489. Actual harm has arisen in the wake of Sonic's data breach regarding its contractual obligations and duties of care to provide security measures to Plaintiffs and the members of the Breach of Implied Contract and Negligence Classes. Further, Plaintiffs and the members of the Breach of Implied Contract and Negligence Classes are at risk of additional or further harm due to the exposure of their personal information and Sonic's failure to address the security failings that lead to such exposure.

490. There is no reason to believe that Sonic's security measures are any more adequate than they were before the breach to meet Sonic's contractual obligations and legal duties.

491. Plaintiffs, therefore, seek a declaration (1) that Sonic's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Sonic must implement and maintain reasonable security measures, including, but not limited to:

- a. Ordering that Sonic engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Sonic's systems on a periodic basis, and ordering Sonic to promptly correct any problems or issues detected by such third-party security auditors;
- b. Ordering that Sonic engage third-party security auditors and internal personnel to run automated security monitoring;
- c. Ordering that Sonic audit, test, and train its security personnel regarding any new or modified procedures;
- d. Ordering that Sonic segment customer data by, among other things, creating firewalls and access controls so that if one area of Sonic is compromised, hackers cannot gain access to other portions of Sonic's systems;
- e. Ordering that Sonic purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;
- f. Ordering that Sonic conduct regular database scanning and securing checks;

- g. Ordering that Sonic routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and
- h. Ordering Sonic to meaningfully educate its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Sonic customers must take to protect themselves.

**VII. PRAYER FOR RELIEF**

492. WHEREFORE, Plaintiffs, on behalf of themselves and the Classes described above, seek the following relief:

- a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the classes as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Classes requested herein;
- b. A judgment in favor of Plaintiffs and the Class awarding them appropriate monetary relief, including actual damages, punitive damages, statutory damages, , equitable relief, restitution, disgorgement, attorney's fees, statutory costs, and such other and further relief as is just and proper.
- c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;
- d. An order requiring Sonic to pay the costs involved in notifying the Class members about the judgment and administering the claims process;
- e. A judgment in favor of Plaintiffs and the Classes awarding them pre-judgment and post judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and
- f. An award of such other and further relief as this Court may deem just and proper.



**VIII. DEMAND FOR JURY TRIAL**

493. Plaintiffs demand a trial by jury on all triable issues.

Dated: July 27, 2018

Respectfully Submitted,

/s/ William B. Federman

William B. Federman

Carin L. Marcussen

FEDERMAN & SHERWOOD

10205 N. Pennsylvania Ave.

Oklahoma City, OK 73120

Telephone: (405) 235-1560

Facsimile: (405) 239-2112

wbf@federmanlaw.com

clm@federmanlaw.com

*Interim Lead Counsel*

Marc E. Dann (0039425)

Brian D Flick (0081605)

DANNLAW

P.O. Box 6031040

Cleveland, OH 44103

Telephone: (216) 373-0539

Facsimile: (216) 373-0536

notices@dannlaw.com

*Interim Liaison Counsel*

Thomas A. Zimmerman, Jr.

ZIMMERMAN LAW OFFICES, P.C.

77 W. Washington Street, Suite 1220

Chicago, IL 60602

Telephone: (312) 440-0020

Facsimile: (312) 440-4180

tom@attorneyzim.com

Melissa R. Emert  
STULL, STULL, & BRODY  
6 East 45th Street  
New York, NY 10017  
Telephone: (954) 341-5561  
Facsimile: (954) 341-5531  
memert@ssbny.com

Michael Fuller  
OLSEN DAINES  
US Bancorp Tower  
111 Southwest 5th Ave, Suite 3150  
Portland, OR 97204  
Telephone: (503) 201-4570  
Facsimile: (503) 362-1375  
michael@underdoglawyer.com

Miles N. Clark  
KNEPPER & CLARK LLC  
10040 W. Cheyenne Ave., Suite 170-109  
Las Vegas, NV 89129  
Telephone: (702) 825-6060  
Facsimile: (702) 447-8048  
miles.clark@knepperclark.com

*Plaintiffs' Steering Committee*

**CERTIFICATE OF SERVICE**

I hereby certify that on July 27, 2018, a copy of the foregoing was served via ECF upon the following counsel for Defendants:

Kari M. Rollins  
SHEPPARD MULLIN RICHTER &  
HAMPTON LLP  
30 Rockefeller Plaza  
New York, NY 10112  
Telephone: 212.634.3077  
Fax: 917.438.6173  
[krollins@sheppardmullin.com](mailto:krollins@sheppardmullin.com)

Craig C. Cardon  
SHEPPARD MULLIN RICHTER &  
HAMPTON LLP  
1901 Avenue of the Stars, Suite 1600  
Los Angeles, CA 90067  
Telephone: 310.228.3749  
Fax: 310.228.3701  
[ccardon@sheppardmullin.com](mailto:ccardon@sheppardmullin.com)

Liisa Thomas  
David M. Poell  
SHEPPARD MULLIN RICHTER &  
HAMPTON LLP  
Three First National Plaza  
70 West Madison Street, 48th Floor  
Chicago, IL 60602  
Telephone: 312.499.6335  
Fax: 312.499.4731  
[lmthomas@sheppardmullin.com](mailto:lmthomas@sheppardmullin.com)  
[dpoell@sheppardmullin.com](mailto:dpoell@sheppardmullin.com)

David A. Riepenhoff  
Melanie J. Williamson  
FISHEL HASS KIM ALBRECHT  
DOWNEY LLP  
7775 Walton Parkway, Suite 200  
New Albany, OH 43054  
Telephone: 614.221.1216 –  
Fax: 614.221.8769  
[driepehoff@fishelhass.com](mailto:driepehoff@fishelhass.com)  
[mwilliamson@fishelhass.com](mailto:mwilliamson@fishelhass.com)

A copy of the foregoing was served via U.S. Mail, postage pre-paid, return receipt requested upon the following:

George Jepsen  
Connecticut Attorney General  
55 Elm Street  
Hartford, Connecticut 06141-0120

Michelle Seagull  
Connecticut Commissioner of Consumer  
Protection  
450 Columbus Boulevard, Suite 901  
Hartford, Connecticut 06103-1840

Gurbir Grewal  
New Jersey Attorney General  
RJ Hughes Justice Complex  
25 Market Street, Box 080  
Trenton, NJ 08625-0080

Ellen Rosenblum  
Oregon Attorney General  
1162 Court St. NE  
Salem, OR 97301-4096

Bob Ferguson  
Washington Attorney General  
800 5th Ave, Suite 2000  
Seattle, WA 98104-3188

Peter F. Kilmartin  
Rhode Island Attorney General  
150 South Main Street  
Providence, Rhode Island 02903

/s/ William B. Federman

William B. Federman

*Interim Lead Counsel for Plaintiffs*